

Exhibit B - 13

327 Midway Park Drive
St. Augustine, FL. 32084

October 1, 2019

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418



To object, you must send a letter stating that you object to the settlement. Your objection letter must include:

The name of this proceeding Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT (N.D. Ga.) EQUIFAX DATA BREACH CLASS ACTION SETTLEMENT

1. NAME/ADDRESS

Jeffrey Scott Biehl – 327 Midway Park Drive, St. Augustine, FL. 32084 USA

2. Your personal signature (an attorney's signature is not enough);

BELOW SIGNED PERSONALLY

3. A statement indicating why you think that you are a member of the settlement class;

STATEMENT: I have membership in TrustedID Equifax credit monitoring that will expire and have verified that my PII was breached by Equifax and that Equifax did not take necessary actions to protect its servers from the breach

4. A statement with the reasons why you object, accompanied by any legal support for your objection;

STATEMENT and REASONS WHY I OBJECT:

I object to this settlement as it does not fairly and equitably compensate the injured millions (147+ millions) of people who placed their trust and identities in the hands of Equifax who did not properly safeguard the information. (See Appendix for reason for breach. It was the fault of not performing the necessary patch to protect the environment.)

Another reason I believe that Equifax does not deserve to be a business anymore in the United States of America as Equifax did NOT take reasonable care to protect the highly sensitive data that USA citizens have entrusted Equifax to guard. (See details in the Appendix.)

Equifax has lost the trust of millions of people and rightly so. Equifax should be ordered by the Court to be dissolved and banned from operating. All of the leadership should be given a jail sentence of at least 30 days and fined \$1,000,000.00 dollars each to pay the Court for disbursement to the people injured. Their assets should be seized just as drug criminals' assets are seized as necessary to pay the Court.


5. A statement identifying all class action settlements to which you have objected

STATEMENT: In the previous five (5) years; and, I. have not objected to any previous class action settlements at all in the past five years.

6. A statement as to whether you intend to appear at the Fairness Hearing, either in person or through a lawyer, and if through a lawyer, identifying your lawyer by name, address, and telephone number, and four dates between 11/19/2019 and 12/05/2019 during which you are available to be deposed by counsel for the Parties.

STATEMENT: I do not plan to appear at the Fairness hearing in person or through a lawyer. My letter serves as my voice to the Court.

Regards,

A handwritten signature in black ink, appearing to read "Jeff Scott Biehl", written in a cursive style.

Jeffrey Scott Biehl

ATTACHMENT

Missed patch caused Equifax data breach

Apache Struts was popped, but company had at least TWO MONTHS to fix it

By Simon Sharwood 14 Sep 2017 at 02:09

Equifax has revealed that the cause of its massive data breach was a flaw it should have patched weeks before it was attacked.

The company has updated its www.equifaxsecurity2017.com/ site with a new "A Progress Update for Consumers" that opens as follows:

Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.

As the Apache Foundation pointed out earlier this week, it reported CVE-2017-5638 in March 2017. Doubt us? Here's the NIST notification that mentions it as being notified on March 10th.

Equifax was breached in "mid-May" 2017, realised it in July and got around to telling the world in early September. If we take "mid-May" as the 15th of the month, Equifax had nine working weeks in which to apply the patch.

That its data breach was entirely avoidable is not the end of Equifax's woes, as the new Progress Update also reveals that "Due to the high volume of security freeze requests, we experienced temporary technical difficulties and our system was offline for approximately an hour at 5PM ET on September 13, 2017 to address this issue."

The company also appears to have suffered another data breach, this time in Argentina where its Bryan Krebs reports "an online portal designed to let Equifax employees in Argentina manage credit report disputes from consumers in that country was wide open, protected by perhaps the most easy-to-guess password combination ever: "admin/admin."

Source: https://www.theregister.co.uk/2017/09/14/missed_patch_caused_equifax_data_breach/

Equifax Officially Has No Excuse

A patch that would have prevented the devastating Equifax breach had been available for months.

Capping a week of incompetence, failures, and general shady behavior in responding to its massive data breach, Equifax has confirmed that attackers entered its system in mid-May through a web-application vulnerability that had a patch available in March. In other words, the credit-reporting giant had more than two months to take precautions that would have defended the personal data of 143 million people from being exposed. It didn't.

As the security community processes the news and scrutinizes Equifax's cybersecurity posture, numerous doubts have surfaced about the organization's competence as a data steward. The company took six weeks to notify the public after finding out about the breach. Even then, the site that Equifax set up in response to address questions and offer free credit monitoring was itself riddled with vulnerabilities. And as security journalist Brian Krebs first reported, a web portal for handling credit-report disputes from customers in Argentina used the embarrassingly inadequate credentials of "admin/admin." Equifax took the platform down on Tuesday. But observers say the ongoing discoveries increasingly paint a picture of negligence—especially in Equifax's failure to protect itself against a known flaw with a ready fix.

A 'Relatively Easy' Hack

The vulnerability that attackers exploited to access Equifax's system was in the Apache Struts web-application software, a widely used enterprise platform. The Apache Software Foundation said in a statement on Saturday (when rumors swirled that the March Struts bug might be to blame) that, though it was sorry if attackers exploited a bug in its software to breach Equifax, it always recommends that users regularly patch and update their Apache Struts platforms. "Most breaches we become aware of are caused by failure to update software components that are known to be vulnerable for months or even years," René Gielen, the vice president of Apache Struts, wrote.

In this case, Equifax had ample opportunity to update.

"This vulnerability was disclosed back in March. There were clear and simple instructions of how to remedy the situation. The responsibility is then on companies to have procedures in place to follow such advice promptly," says Bas van Schaik, a product manager and researcher at Semmler, an analytics security firm. "The fact that Equifax was subsequently attacked in May means that Equifax did not follow that advice. Had they done so this breach would not have occurred."

More Equifax

Penetration testers and other security researchers say that it would have been simple for an attacker to exploit the flaw and get into the system. "Once they identified Equifax's systems as vulnerable, actually exploiting the vulnerability to gain access to the Equifax servers and network will unfortunately have been relatively easy," says van Schaik, who recently discovered and disclosed a different Apache Struts bug. "It's hard to say how difficult it will have been for the attackers to get their hands on customer data once they found their way into Equifax's servers and network. But the timeline suggests that time was on the attackers' side."

After exploiting the vulnerability to gain a foothold, the attackers may have found scores of unprotected data immediately or may have worked over time—between mid-May and the end of July—to gain more and more access to Equifax's systems. "Generally when you successfully exploit a web-application bug like this you will become the system user who owns the web server process," says Alex McGeorge, the head of threat intelligence at the security firm Immunity. "Security best practices dictate that this user have as little privilege as possible on the server itself, since security vulnerabilities in web applications and web servers are so commonly exploited." In practice, though, McGeorge says that hackers could have found credentials or other information in plaintext right away if Equifax didn't have proper protections in place.

Mounting Concerns

The company's attempts at damage control have been boilerplate at best. "Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted," the company said in a statement Wednesday. "We continue to work with law enforcement as part of our criminal investigation."

Most Popular

Lawmakers are planning two hearings to scrutinize the situation, though, and have requested detailed information about the breach from Equifax. Dozens of people whose personal data was exposed have already filed lawsuits against the company. Peter Kaplan, the acting director of public affairs at the Federal Trade Commission, told WIRED in a statement that "the FTC typically does not comment on ongoing investigations. However, in light of the intense public interest and the potential impact of this matter, I can confirm that FTC staff is investigating the Equifax data breach." And politicians have additionally called on federal watchdog and protection agencies like the Securities and Exchange Commission and the Consumer Financial Protection Bureau to initiate their own investigations.

Equifax will suffer scrutiny and losses because of the breach, but the real victims are the individuals whose data was potentially compromised. And Equifax has particular responsibility to protect its consumer data, since much of it doesn't even come from customers who directly choose to do business with the firm, but surfaces instead from credit check requests for anyone living and working in the US. "I am concerned," Immunity's McGeorge says. "This is a thing that you use whether you realize it or not, because all commerce data goes through them. You do have a stake in this."

Source: https://www.wired.com/story/telltale-heart-fitbit-murder/#intcid=recommendations_wired-right-rail-popular_f02748f7-333a-48c7-9d61-ecd807daebc7_cral-top3-1

327 Midway Park Drive
St. Augustine, FL. 32084

Equifax Data Breach Class Action Settlement
Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

This packaging is the property of the U.S. Postal Service® and is provided solely for use in sending Priority Mail® shipments. Misuse may be a violation of Federal Law. Please do not reuse. © 2013 U.S. Postal Service. All rights reserved.

PRIORITY MAIL
POSTAGE REQUIRED

9405 5102 0083 0363 7903 64



USPS TRACKING #

SHIP TO:
Equifax Data Breach Class Action Settlement
ATTN: Objection C/O JND Legal Admin
PO BOX 91318
ADMINISTRATOR
SEATTLE WA 98111 - 9418

OCT 07 2019

Shipped using PostalMate
Pkg:163318

Christie Biehl
327 MIDWAY PARK DR
ST AUGUSTINE FL 32084

OCT 07 2019

B900 0021

PRIORITY MAIL 2-DAY

Endicia
Paid 156297-435 RRDE EXP 05/20

071V01329336



CID: 166426
CommercialPlusPrice

US POSTAGE AND FEES PAID
PRIORITY MAIL
Oct 05 2019
Mailed from ZIP 32084
PM Flat Rate Env

P

PRESS FIRMLY TO SEAL

**PRIORITY®
★ MAIL ★**

- DATE OF DELIVERY SPECIFIED *
- USPS TRACKING™ INCLUDED *
- INSURANCE INCLUDED *
- PICKUP AVAILABLE
* Domestic only

WHEN USED INTERNATIONALLY,
A CUSTOMS DECLARATION
LABEL MAY BE REQUIRED.

EP14B July 2013 OD: 10 x 6



PS00001000012



This envelope is made from post-consumer waste. Please recycle - again.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

November 10, 2019

Richard B. Russell Federal Building
2211 United States Courthouse
75 Ted Turner Drive, SW
Atlanta, GA 30303-3309

FILED IN CLERK'S OFFICE
U.S.D.C. - Atlanta

NOV 20 2019

JAMES N. HATTEN, Clerk
By:  Deputy Clerk

Dear Honorable Chief Judge Thomas Thrash Jr.,

I am writing to object to the proposed settle between the FTC and Equifax. I believe some of the terms are too ambiguous and need more details so victims can make well informed decisions. I think some of the terms are too shallow and don't provide enough consideration for victims. Finally, I feel some problems received no treatment but need to be addressed.

Equifax had the opportunity to protect the data for a fraction of the cost but the company squandered it. After reading the settlement and some of the artificially small caps on payments for services and costs I developed the impression the company is trying to push most of the risk and loss onto victims and tax payers. I sincerely hope the government is wise to what is going on here.

If the Court is not aware of the problems and challenges victims of a data breach face, then I respectfully recommend *Identity Theft in Maryland: Shifting Circumstances – Continuing Challenges*.¹ It is written by the former Attorney

¹ http://dls.state.md.us/data/polanasubare/polanasubare_coucrijuscivmat/Identity-Theft-2013.pdf

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

General of Maryland and is one of the more comprehensive treatments I have read. From the document:

Criminals are using PII, however, not just to steal money but to steal health care, prescription drugs, citizenship status, tax refunds, unemployment benefits, and even driving privileges. A relatively recent disturbing trend is the commission of identity fraud to avoid sex offender registration requirements.

Background

The Equifax data breach occurred mid-May to July 2017, and was announced September 2017². Visa and Mastercard reported the suspicious activity as early as late 2016.³ The breach affected approximately 147 million individuals. The breach was attributed to an unpatched server. In particular, Apache Struts Vulnerability CVE-2017-5638. The vulnerability was disclosed in March 2017.

Many people in my field of Information Security were surprised Equifax was not patching their servers in a timely manner. Patching servers with security updates like for CVE-2017-5638 is “System Administration 101.” All levels of system administrators are taught number one threat to an organization’s data is unpatched servers. Even junior administrators know to patch their servers

After the breach but before it was disclosed some officers of the company “doubled down” on illegal activity and sold some their shares in the company to

² <https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/>

³ <https://krebsonsecurity.com/2017/09/equifax-hackers-stole-200k-credit-card-accounts-in-one-fell-swoop/>

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

avoid the upcoming losses. At least one was charged with insider trading and is serving prison time for it.⁴

According to FTC statistics, identity theft complaints declined in 2016⁵, but rose 14% in 2017⁶ and rose an additional 24% in 2018⁷. Statistics indicate information from the Equifax data breach is actively being used by bad actors.

While there were a number of breaches in 2017, the majority of them did not include names and social security numbers. And those that included names and social security numbers did not achieve the magnitude of the Equifax breach. The second through fourth place finishers are America's JobLink, 4.8 million records; TIO Networks, 1.6 million; and Washington State University, 1 million records. Equifax contributed over 92% to the records lost social security records in 2017. Combined, the runner's up account for less than 5% of the records lost social security records in 2017.

Ambiguous Terms

The terms of the settle agreement are ambiguous. There are several instances of ambiguity that should be fixed before proceeding with the settlement.

First, the length of credit monitoring is variable. It could be as little as 4 years or could be as long as 10 years. If more people opt for the credit monitoring than anticipated, then more money needs to be added to the fund. The length must be

⁴ <https://www.justice.gov/usao-ndga/pr/former-equifax-employee-sentenced-insider-trading>

⁵ <https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints>

⁶ <https://www.ftc.gov/news-events/press-releases/2018/03/ftc-releases-annual-summary-complaints-reported-consumers>

⁷ <https://www.ftc.gov/news-events/press-releases/2019/02/imposter-scams-top-complaints-made-ftc-2018>

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

fixed and clearly stated. Otherwise consumers do not know what they may receive.

Second, the monetary compensation option is variable. It could be as much as \$125 USD or as little as a few dollars. If more people opt for the monetary compensation than anticipated, then more money needs to be added to the fund. The dollar amount must be fixed and clearly stated. Otherwise consumers do not know what they may receive.

Third, the settlement does not specify the details of monitoring. It is not clear what Equifax, Experian, and TransUnion will monitor, and what will be provided to a victim in the report. It is also not clear how some things are going to be monitored.

An example of “how something is going to be monitored” is a bank account. Bank accounts are fundamental and most people have them. However, banks don’t submit customer information or checking and savings account information to reporting agencies. The reason is simple – the banks don’t want their customers poached by a competitor. There is no mechanism in the current settlement to detect unauthorized bank accounts.

Now suppose bad checks are written on the fraudulent bank account. Credit reports don’t include bounced check information. There is no mechanism in the current settlement to detect bounced checks from fraudulent bank accounts.

So it is not clear to me how a victim will find out about additional bank accounts and bad checks given the monitors don’t receive the information. There is a way to do detect the fraud in many cases, but the option is not available in the

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

settlement. In fact, Wells Fargo exploited this fact and opened fake bank accounts using their banking customer's identities.⁸

In an effort to remove confusion and ambiguity, Walton wrote to the FTC in October and asked for details of what was being monitored and exemplary reports from the agencies. Walton also asked the items be submitted with the settlement for the Courts approval. Walton was directed to the Equifax Data Breach FAQ⁹ which lacked the information. The Administrator's site also lacked the information. The information also was not provided to the Court for approval.

To put the problem of ambiguous terms in perspective: would the Judge, the FTC lawyers or the Equifax lawyers agree to a mortgage or credit card if the term was "some interest rate" and subject to change at any time? I'm guessing no. I'm speculating attorney would want an exact interest rate with exact terms stated up-front and in writing.

Credit Monitoring

The settlement claims to offer "Up to 10 years of free credit monitoring", and also states "at least four years of free monitoring of your credit report at all three credit bureaus."¹⁰ There are several problems with these terms.

First, the bad actors who are using the stolen identities do not observe "4 year rule" or the "10 year rule". The bad actors will commoditize the stolen identity as long as it is bearing fruit. A victim who is being actively exploited needs a lifetime of protection.

⁸ <https://www.forbes.com/sites/maggiemcgrath/2016/09/08/wells-fargo-fined-185-million-for-opening-accounts-without-customers-knowledge/>

⁹ <https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement>

¹⁰ <https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement#FAQ5>

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

Second, the term assumes bad actors will use the stolen identity immediately. Economic theory tells us if too many stolen identities are dumped on the market at once, then the value (price) for a stolen identity will drop. I believe the thieves will keep the value (price) for a stolen identity high, so they will limit the rate that stolen identities are released and used. The FTC statistics seem to indicate this pattern since identity theft complaints are growing more than expected over time. A potential victim who could be exploited needs a lifetime of protection.

Interestingly, baseball player agents recognized the same economic pressures as the data thieves, and that is why collective bargaining in baseball does not allow a player to enter free-agency until 3 years. Agents realized too many super-star free agents hitting the market too frequently will drive down the cost of the player.

Third, some victims are infants and children. They will not learn of the damage caused by the data breach until long after the 4 years or 10 years have expired. A victim who is being actively exploited or potential victim who could be exploited needs a lifetime of protection. A child victim who could be exploited needs a lifetime of protection.

Fourth, the Fair Credit Reporting Act (FCRA) cited in the settlement allows derogatory entries on a credit report for 7 or 10 years. The settlement only ensures up to four years of monitoring. There is a six year gap that needs to be closed based on Congress' rendering of interstate commerce laws in this area.

Breach Disclosure

The Equifax data breach is unique in that a credit reporting agency suffered the breach. Equifax controls their database and can place entries in their database at

FEDERAL TRADE COMMISSION V. EQUIFAX INC.

Case 1:19-cv-03297-TWT

will¹¹. The settlement does not require Equifax to report the stolen identity event on the consumer's credit report. There are several problems with the missing information.

First, the lack of an "Equifax 2017 data breach" entry means an individual's credit report is incomplete and does not paint an accurate picture of the individual. Known information is being intentionally omitted. Companies and agencies that receive the reports cannot use the information to assess an individual for credit worthiness, assess an individual for employment, or assess an individual for insurance because the information is missing.

Put another way, a fully qualified individual may be disqualified because of an unexplained derogatory entry due to an identity theft incident. The receiver of the credit report is no wiser and interprets the entry against the victim because necessary information is missing from the report.

As a concrete example, suppose the stolen information is used to open a checking account and attend a doctor's visit. Further, suppose the identity thief writes a bad check at the doctor's office. A credit report won't report the bank account and won't report the bad check. However, a collection agency could report the unpaid medical bill and subsequent debt collection. The events will negatively affect the individual even if the events took place 2500 miles away from the victim.

And god save the individual if he or she is a candidate for a law enforcement position, a sensitive military MoS, or a top secret clearance; and the doctor's visit

¹¹ In contrast the Anthem data breach, which was another massive breach, did not have this unique facet. Anthem did not control credit reporting databases, and could not compel credit reporting agencies to report the incident on a consumer report.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

was for a venereal disease or drug overdose or something similarly distasteful. A thorough background check will uncover these fallacious facts, and it won't be obvious to the investigator that these facts are actually false and part of an identity theft. A victim trying to explain this to an investigator is too late. It needed to be fixed before the investigation.

Second, the missing "Equifax 2017 data breach" entry means an individual must be aware of a derogatory entry from the breach before it can be fixed or explained. This places an individual at a disadvantage in the market by default. Here, the market could be any market like home loan, credit card rate or job market. Being disadvantaged "out of the box" is simply unfair to the individual.

Third, every individual affected by the report must write to Equifax every three months and request that their credit report include the information. A victim should not have to do anything special; the protection and entry should simply be present. It is not clear to me if a credit reporting agency like Equifax will honor such a request like "Please include the statement, I was part of the Equifax Data breach in 2017 and my identity may be used fraudulently" if it is not mandated by the settlement. It is a burden the victims should not have to endure.

Fourth, the cash portion of the settlement has been reduced to proverbial pennies. Individuals who have to manually tend to this task will never be compensated for their time. In fact, the cash portion of the settlement is so small it may not even cover the cost of the postage stamps over time.

Finally, if Equifax claims to provide accurate information about an individual but fails to supply "Equifax 2017 data breach" entry in the report, then the information about an individual is incomplete and not accurate.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

Missing Agencies

The settlement names three agencies for credit monitoring: Equifax, Experian, and TransUnion. The three credit reporting agencies have a limited looking glass and depend on other firms and institutions to feed the agencies data. If an agency lacks an appropriate data source then some information is unreported.

There are other agencies that perform better in certain areas of monitoring. For example Early Warning is credit reporting agency that is not on the list. Early Warning is a collection of the largest US banks that pool their customer databases and provide real-time risk management for financial transactions. If a bank account or credit card exists for a stolen identity – or an application is made for a bank account or credit card – then there is a good chance Early Warning will know about it and the three credit reporting agencies **will not** because Early Warning does not share the bank data.

It would benefit victims of the breach to obtain their Early Warning credit reports on a regular basis because Early Warning provides information not available to the three credit reporting agencies.

Summary Reporting

Credit reporting agencies like Equifax, Experian, TransUnion and Early Warning prepare different reports for different applications and different customers. Painting with a broad brush there are at least two types of reports: summary reports and detailed reports.¹²

¹² “Summary report” and “detailed report” is the exact language used by Early Warning.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

Victims in this settlement will receive a quasi-summary report.¹³¹⁴¹⁵ Lenders, employers, law enforcement agencies, the military and insurers will often receive detailed reports. The disparity has several problems for victims.

First, the victims are provided different reports than others that request the reports, like law enforcement and background investigators. A summary report provided to the victims will lack information present on the detailed report seen by lenders, employers, law enforcement, military, insurers, etc.

Second, since victims have an abridged view of their information, and they may not have the opportunity to correct the incomplete, inaccurate or incorrect information. They may not even know there is a problem. A victim cannot correct what they don't know about.

Third, most people do not know there are different reports, and so they don't know to ask for the detailed or comprehensive report. In the case of Equifax, Experian, TransUnion, their example reports are summary reports with some details; and not detailed reports provided to lenders, employers, law enforcement, military, insurers, etc.¹⁶¹⁷¹⁸

In fact it is a practice at Early Warning to provide a summary report when someone asks for his or her credit report. The only time a person receives a detailed report is when they specifically ask for it.

¹³ https://www.equifax.com/pdfs/corp/Equifax_Optima_Sample_Report.pdf

¹⁴ https://www.experian.com/credit_report_basics/pdf/samplecreditreport.pdf

¹⁵ https://www.transunion.com/docs/rev/personal/Credit_Report_Explanations.pdf

¹⁶ https://www.equifax.com/pdfs/corp/Equifax_Optima_Sample_Report.pdf

¹⁷ https://www.experian.com/credit_report_basics/pdf/samplecreditreport.pdf

¹⁸ https://www.transunion.com/docs/rev/personal/Credit_Report_Explanations.pdf

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

Early Warning is not alone. Equifax, Experian, and TransUnion's stock request form does not request the detailed or comprehensive report. It does not matter whether a consumer orders over the phone or sends the form by mail. The process does not offer the detailed report, so there is no way for a consumer to request the detailed report.

Disparity among Members

The settlement action covers roughly 147 million people in the United States. Unfortunately all class members are not treated equal. Credit Bureaus maintain "VIP Databases" of influential members of society. Influential members of society include politicians, judges, athletes, actors, actresses and musicians.

The reporting agencies **voluntarily** provide special treatment for the influential members of our society. Derogatory items are manually checked and confirmed, some derogatory items are not reported on an individual's credit report, and other derogatory information is removed from a credit report. In contrast most class members are not in the VIP database, they do not enjoy preferential treatment, and they are subject to unconfirmed reporting complete with the inaccuracies that follow. There are several problems here.

First, the credit bureaus give special treatment to VIP members for a reason. They want to ensure the status quo. Reporting agencies don't want to risk the ire of politicians who could write legislation against them. And they don't want athletes, actors and actresses taking up causes on social media which could lead to unwanted change in their business.

The bigger problem is, the agencies are perverting the political process and denying most members of society and all members of the class their due process.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

Some might even say the agencies are corrupting and influencing influential members of society.

The practice of influencing certain members of our society must stop so that all members of society and the class can enjoy the benefits of unbiased legislation and meaningful protections.¹⁹ The settlement agreement must stop the practice of influencing like this.

Second, all members of the class should receive the same treatment. I don't want to ask the court to dismantle the VIP database or the processes involved in maintaining the database. It is good the processes are in place, and it is good at least some individuals receive good care in these matters. Instead, I would like the settlement to ensure every individual receives the same handling as politicians, judges, athletes, actors, actresses and musicians. And as with influential members of society, all class members should enjoy the protections for life at no charge.

I first learned of the VIP databases years ago. I believe I was watching a financial crisis documentary. Bill Black was interviewed and spilled the beans on the VIP databases. I encourage the Court to discuss this further with Dr. William Black, J.D.²⁰ He can be found teaching at the University of Missouri.

Privacy

Members of the class must provide identifying information to enroll in the services stated in the settlement. The identifying information includes name,

¹⁹ The Electronic Frontier Foundation has several good position papers on this problem. The EFF does not directly attack the VIP databases. Rather, they discuss the gaps caused by inadequate legislation.

²⁰ Dr. Black is a J.D. and a professor of law at the University of Missouri. He is a former bank regulator and helped prosecute the folks responsible for the financial crisis in the mid-1980's, like Charles Keating. The US government declined his assistance after the 2008 meltdown. Not surprising, no criminal prosecutions were attempted in the US for the folks who were responsible for the melt down.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

social security number, address, phone number and email address. The reporting agencies may not have up-to-date information on an individual so this is a proverbial “gold mine” of information.

The problem is, some individuals may wish to remain private. Individuals in this group would include people who value their privacy, individuals who shun the practices of modern data collection, and individuals who are used to strong privacy protections, like those provided in European nations. It is tenuous to blame someone for not wanting to share their information in this instance. Information sharing is what got them here in the first place. Once bitten, twice shy, as the saying goes.

The settlement does not appear to place any restrictions on how the information is used after the victim identifies himself or herself. The settlement must ensure the personal information gathered for the purposes of the settlement remain private; and the information is not shared, sold or disseminated in any way.

Barriers to Service

I can relay this problem with firsthand experience. My apologies for the verbosity in this section. Credit reporting agencies place too many barriers and deny credit report requests by individuals.

In 2005 I was in a hit-and-run motorcycle accident. I was the motorcyclist. I had medical insurance and short term disability, but I did not have long term disability. I was out of work about two years while my back healed. My last surgery occurred in 2006 or early 2007, but were paid for by insurance.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

During the two year time a credit card and loan were charged off. I had rainy day money but I used it to live on rather than pay bills. I accepted the events as "shit happens, and sometimes it happens to you."

In 2014 I failed to obtain a particular job I was very interested in. I performed a root cause analysis and concluded I needed more information to explain the events. My charge off occurred about a decade earlier so the charge-off should not have factored into the failed attempt due to limitations specified by FCRA.

I attempted to obtain my credit report from Equifax in June 2014. I first tried by phone and was denied by the automated phone system. I then tried in writing using the form from the Equifax website but the request was not fulfilled. Equifax did not bother sending me a denial letter. They simply did not respond.

Equifax does not have an office in my state so I could not visit a local office, show my driver's license or passport, and obtain the consumer report. Equifax does not provide a number to talk to a real person so I could not get more information from the company.

I suppose my next step was hire a lawyer and initiate an action in Federal Court. This is not a reasonable course of action for a reasonable person. Reasonable people accommodate reasonable requests, and reasonable people don't expect to spend \$10,000 USD to retain a lawyer to obtain a credit report guaranteed by Federal law.

There were too many barriers in the process.

Removing the barriers means a person can get to a local office, show identification, and obtain a detailed credit report from the office. For accessibility

FEDERAL TRADE COMMISSION v. EQUIFAX INC.

Case 1:19-cv-03297-TWT

purposes, it does not matter if the credit agencies open several local in each state. Or a victim can use a designated agent of a reporting agency to fulfill the request. The point is, there is a local place to go to obtain the report and talk to a real person if needed.

If the Court believes a victim will be able to easily obtain a credit report then it is probably mistaken. The settlement must ensure barriers are removed so victims can obtain a report in a timely manner.

SIRF Fraud

A byproduct of the data breach is identity theft and Stolen Identity Refund Fraud (SIRF)²¹. City, state and federal governments and tax payers are absorbing the costs associated of this data breach.

As the 9th Circuit Court of Appeals correctly recognized there is a “credible threat of real and immediate harm” after a data breach. The FTC statistics confirm the 9th Circuit Court of Appeals’ intuition. As reported by the FTC, something reversed the decline in identity theft complaints for 2016 and caused the 14% rise in 2017 and 24% rise in 2018. It was most likely the Equifax data breach since Equifax was responsible for over 92% of the social security numbers lost in 2017; and there are no other credible sources or explanations.

According to US Treasury, the United States losses over \$6 Billion USD a year in SIRF fraud²². The increased losses due to SIRF fraud for 2017 and 2018 were passed on tax payers. There are approximately 329 million people in the United States. 147 million or 44.6% are members of this class settlement.

²¹ <https://www.justice.gov/tax/stolen-identity-refund-fraud>

²² Treasury reports losses of over \$30 billion per year, but claims to recover over 80% of the losses

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

It appears the FTC did not study the problem or provide an explicit solution. Not collecting data and pretending a problem does not exist is disingenuous and unethical at best. I have stronger opinions on the matter, but I am going to keep them to myself. The Court needs complete and accurate information to evaluate the settlement, but it is completely missing here.

Correlating lost identity information from Equifax with SIRF fraud from Treasury is as simple as a database query. For each victim of the breach, report the dollar amount of the SIRF fraud in 2016 (pre-breach), 2017 and 2018 (post-breach).²³ Remove from the list anyone who was fraudulently active in 2016, or part of another breach like America's JobLink.

I believe the Court's ruling on the City of Chicago intersects here. If I am not misunderstanding the court's ruling, governments like the City of Chicago are part of this settlement and they have to make their claims as part of this settlement. Therefore, issues like SIRF fraud, loss of revenue and unfunded services needs to be addressed now for city, state and federal governments.

Data breaches in the private sector assign blame and hold the appropriate parties responsible. For example, Home Depot settled with banks for bank's losses due to the Home Depot data breach.²⁴ Tax payers, members of the class and government expect the same of Equifax. Equifax must take financial responsibility for the SIRF fraud and financial hardships it has caused.

²³ If my estimates are correct, tax payers and class members will pay out more for SIRF fraud then they will get back from the this settlement. It is a net loss for tax payers and class members.

²⁴ <https://fortune.com/2017/03/09/home-depot-data-breach-banks/>

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

I generally don't make demands but I will in this case. I demand the FTC study the problem and release the "uncooked" statistics as part of the settlement. The statistics must anonymized information and include exact dollar amounts.

Profiteering

Equifax is one of the companies that provides risk management services to various treasuries and comptrollers offices, at both the state and federal levels. In the case of the Equifax data breach, the company introduced the disease and are now selling the cure.

My research indicates the names, addresses and social security numbers of victims were **not** provided to treasury and comptroller offices. State and federal agencies lacked critical information and were not able to place alerts on victim accounts nor monitor the accounts with heightened vigilance. Instead Equifax is selling the information as a service to the state and federal governments.

This is not the only instance of Equifax profiteering. The company charged consumers for credit freezes through November 2017.²⁵ I am appalled the company was allowed to charge consumers for protections needed due to the company's own mistakes.

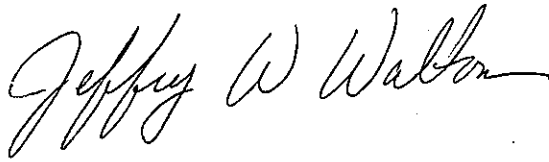
A settlement must eliminate the profiteering.

Closing

Thank you for reading this objection letter. I hope my concerns can be addressed.

²⁵ <https://www.nytimes.com/2017/09/12/your-money/equifax-fee-waiver.html>

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

A handwritten signature in black ink, reading "Jeffrey W. Walton". The signature is written in a cursive, flowing style.

Jeffrey Walton

8482 Fort Smallwood Road

Unit B-103

Pasadena, MD 21122



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Equifax Data Breach Settlement

Share This Page

September 2019

Affected by the Equifax breach? File a claim now.

In September of 2017, Equifax announced a data breach that exposed the personal information of 147 million people. The company has agreed to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. The settlement includes up to \$425 million to help people affected by the data breach.



If your information was exposed in the data breach, you can file a claim at [EquifaxBreachSettlement.com](https://www.equifax.com/settlement) for the benefits described below.

Not sure if your information was exposed? Use this [look-up tool](#) to see.

You can [file a claim](#) for:

Free Credit Monitoring and Identity Theft Protection Services

- Up to 10 years of free credit monitoring, including:
 - At least four years of free monitoring of your credit report at all three credit bureaus (Equifax, Experian, and TransUnion) and \$1,000,000 of identity theft insurance.
 - Up to six more years of free monitoring of your Equifax credit report.
(Previously, a cash payment was identified as an alternative to the free credit monitoring, but there are limited funds available. See [FAQ 4](#) for details.)
- If you were a minor in May 2017, you are eligible for a total of 18 years of free credit monitoring.

Cash Payments (capped at up to \$20,000 per person)

- For expenses you paid as a result of the breach, like:
 - Losses from unauthorized charges to your accounts
 - The cost of freezing or unfreezing your credit report
 - The cost of credit monitoring
 - Fees you paid to professionals like an accountant or attorney
 - Other expenses like notary fees, document shipping fees and postage, mileage, and phone charges
- For the time you spent dealing with the breach. You can be compensated up to \$25 per hour up to 20 hours. There are limited funds available so your claim may be reduced. See [FAQ 7](#) for more details.
 - If you submit a claim for 10 hours or less, you must describe the actions you took and the time you spent doing those things.
 - If you claim more than 10 hours, you must describe the actions you took AND provide documents that show identity theft, fraud, or other misuse of your information.
- For the cost of Equifax credit monitoring and related services you had between September 7, 2016, and September 7, 2017, capped at 25 percent of the total amount you paid.

Even if you do not file a claim, you can get:

Free Help Recovering from Identity Theft

- For at least seven years, you can get free identity restoration services. If you discover misuse of your personal information, call the settlement administrator at 1-833-759-2982. You will be given instructions for how to access free identity restoration services.

Free Credit Reports for All U.S. Consumers

- Starting in 2020, all U.S. consumers can get 6 free credit reports per year for 7 years from the Equifax website. That's in addition to the one free Equifax report (plus your Experian and TransUnion reports) you can get at [AnnualCreditReport.com](https://www.annualcreditreport.com). [Sign up for email updates](#) to get a reminder in early 2020.

FAQs

1. [What is the deadline to file a claim?](#)
2. [When will I get my benefits?](#)
3. [How will I get my benefits?](#)
4. [I thought I could choose \\$125 instead of free credit monitoring. What happened?](#)
5. [I don't want Equifax to have my data. What can I do?](#)

6. I don't want credit monitoring from Equifax. What are my options?
 7. How much of the settlement fund can be used to pay claims for time spent dealing with the data breach?
 8. I'm not sure I was affected by the data breach. How can I find out?
 9. What else can I do?
-

1. What is the deadline to file a claim?

You must file a claim by January 22, 2020.

2. When will I get my benefits?

The settlement administrator will not send out any benefits until they are allowed to do so by the court, which will be **January 23, 2020, at the earliest**. We will update this page, and send email updates, when we have more information.

3. How will I get my benefits?

For free credit monitoring, after final approval from the court, you will get an activation code with instructions. You can choose to receive this code by email or postal mail when you file your claim.

For cash payments, you can choose to get a check or debit card when you file your claim. It will be sent to your mailing address after final approval from the court.

4. I thought I could choose \$125 instead of free credit monitoring. What happened?

The public response to the settlement has been overwhelming. Because the total amount available for the alternative compensations is \$31 million, each person who takes the money option is likely to get a very small amount. Nowhere near the \$125 they could have gotten if there hadn't been such an enormous number of claims filed.

The free credit monitoring provides a much better value, and everyone whose information was exposed can take advantage of it. If your information was exposed in the data breach, and you file a valid claim before the deadline, you are **guaranteed** at least four years of free monitoring at **all three credit bureaus** (Equifax, Experian, and TransUnion) and \$1,000,000 of identity theft insurance, among other benefits. The market value of this product is hundreds of dollars per year.

You can still choose the cash option on the claim form, but you will be disappointed with the amount you receive and you won't get the free credit monitoring.

5. I don't want Equifax to have my data. What can I do?

Related News

- [FTC Encourages Consumers to Opt for Free Credit Monitoring, as part of Equifax Settlement](#)
- [Equifax to Pay \\$575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach](#)



[ftc.gov](https://www.ftc.gov)

NOVEMBER 12, 2019

eff.org



Equifax Data Breach Update: Backsliding

After Equifax's calamitous 2017 data breach, its settlement with the Federal Trade Commission (FTC) and the private attorneys representing victims appears to offer two potential remedies to all 147 million American consumers affected: free credit monitoring, or if individuals already had free credit monitoring, an up to \$125 cash payment. The FTC directed consumers affected by the breach to a third-party website where they could quickly and easily file their claim.

At the time, EFF tepidly commented on the settlements' efforts to compensate consumers. But we also noted that the \$125 payments would come from a \$31 million fund, meaning that if all 147 million victims chose the payment, each person's payment would be reduced on a *pro rata* basis to as little as 21 cents each.

Indeed. Less than one week after it announced the settlement, the commission began encouraging consumers to forego the monetary compensation in favor of free credit monitoring, even if they *already* had it. In a blog post, the FTC told consumers that, because an "unexpected number" of victims filed claims, "each person who takes the money option will wind up only getting a small amount of money. Nowhere near the \$125 they could have gotten if there hadn't been such an enormous number of claims filed."

The government apparently failed to anticipate that, out of 147 million Americans victims, more than the maximum 248,000 who could have claimed their \$125 without reducing the award given to each person would have opted to do so. Even worse, it instituted a variety of new burdensome,

Case 1:19-cv-03297-TWT

bureaucratic steps required to claim the monetary award to nudge victims away from financial compensation.

Consumers should not have to jump through hoops to receive compensation for serious data privacy harms. The “unexpected” number of claimants in this case should strongly signal to policymakers that Americans care about the security of their personal data. Consumers intuitively know what EFF has said all along: the companies that store consumer’s personal information—often without their knowledge—have an obligation to protect it. If they don’t, they should pay for the harm that ensues. And financial penalties should be high enough to incentivize better data privacy practices in the future.

This settlement ensures neither. While it’s easy to be angry at the FTC, the problem really lies with the current state of privacy law. We have said it before and will say it again: without new privacy laws, or a change in how the courts view those harms, companies will not adequately invest in consumer privacy protection.

If Congress wants to protect consumer privacy, it should enact legislation with the following rules and protections.

Information fiduciary and national data breach notification rules

This one is simple: companies that collect your personal information should have a legal duty to protect it. A strong information fiduciary law would require that companies follow best practices and exercise care to protect user information as a matter of course—not as a negotiated settlement years later.

Private right of action and real damages

We need to ensure a direct, private cause of action for data breaches and other digital privacy harms to give victims a more reasonable day in court than they have now. Because data harms can be hard to quantify financially, the law should provide statutory or liquidated damages, like it does for illegal wiretapping, where Congress long ago recognized that there should be no requirement to show financial harm in order to recover.

Data broker registration

Data brokers harvest and monetize our personal information without our knowledge or consent. Worse, many data brokers fail to securely store this sensitive information, predictably leading to data breaches. One good way to facilitate better oversight comes from Vermont's new data privacy law, which requires data brokers to register annually with the government.

Non-discrimination rules

Pay-for-privacy is unfair. The law should prohibit companies from denying services, charging different prices, providing different quality levels, or otherwise discriminating against users who choose more private options.

Stronger rule-making authority for the FTC

Federal regulators must have the authority and funding to write and enforce consumer privacy rules. Congress should empower the FTC—an expert agency once tasked with data privacy regulation—to set and enforce sound security standards.

No federal pre-emption

Federal law should set a floor—not a ceiling—for privacy protection. States, as our “laboratories of democracy,” must retain their power to respond to technological changes and constituent concerns by enacting innovative data security policies.

No new criminal liability

And finally, one thing to avoid: existing computer crime laws are already extremely unfair and overbroad. That causes real harm and injustice. It also threatens the very security researchers—like the one who found an Equifax bug before the breach—who work to protect the rest of us. Any new efforts to address data breaches should focus on incentives to protect data rather than further expanding criminal liability for coders.

It has become increasingly clear that the Equifax settlement is inadequate for both compensating victims and preventing future harms. But future settlements won't be better without changes in the law or in how courts treat privacy harms. U.S. privacy law does not even give FTC the power to

require direct compensation to consumers—a powerful way to make companies pay consumers for the harm they caused. The FTC only secured it this time because individual suits were joined to its actions. Bottom line: we can't expect the current, limited-power FTC to clean up the messes created by our failure to require stronger data protections.

Our legislators have an obligation to enact the stronger data privacy protections that their constituents want and deserve.

Note: Thanks to EFF Legal Intern Victoria Noble for help with this update.

JOIN EFF LISTS

Join Our Newsletter!

Email updates on news, actions, events in your area, and more.

Email Address

Postal Code (optional)

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:



RELATED UPDATES

Federal Court Rules Suspicionless Searches of Travelers'



PRESS RELEASE | NOVEMBER 12, 2019

Phones and Laptops Unconstitutional

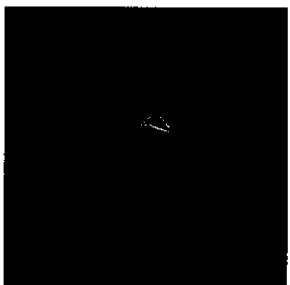
BOSTON—In a major victory for privacy rights at the border, a federal court in Boston ruled today that suspicionless searches of travelers' electronic devices by federal agents at airports and other U.S. ports of entry are unconstitutional. The ruling came in a lawsuit, *Alasaad v. McAleenan*, filed by...



PRESS RELEASE | NOVEMBER 12, 2019

EFF Sues DHS to Obtain Information About the Agency's Use of Rapid DNA Testing on Migrant Families at the Border

San Francisco—The Electronic Frontier Foundation (EFF) sued the Department of Homeland Security (DHS) today to obtain information that will shine a light on the agency's use of Rapid DNA technology on migrant families at the border to verify biological parent-child relationships. In a Freedom of Information Act (FOIA) complaint filed...

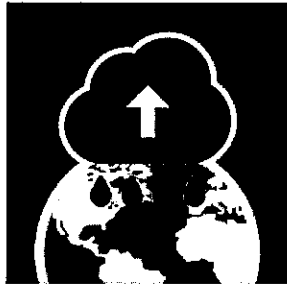


DEEPLINKS BLOG BY GENNIE GEBHART, EVA GALPERIN | NOVEMBER 6, 2019

FTC Takes Action Against Stalkerware Company Retina-X

The FTC recently took action against stalkerware developer Retina-X, the company behind apps Flexispy, PhoneSheriff, and Teenspy. The FTC settlement bars Retina-X from distributing its mobile apps until it can adequately secure user information and ensure its apps will only be used for "legitimate purposes." But here's...

Congress, Remember the 4th Amendment? It's Time to Stop the U.S.-UK Agreement.



DEEPLINKS BLOG BY JOE MULLIN | NOVEMBER 4, 2019

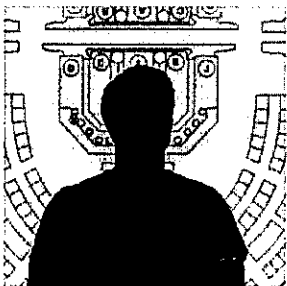
Unless Congress stops it, foreign police will soon be able to collect and search data on the servers of U.S. Internet companies. They'll be able to do it without a probable cause warrant, or any oversight from a U.S. judge. This is all happening because of a new law enforcement...



DEEPLINKS BLOG BY ADAM SCHWARTZ | OCTOBER 30, 2019

Strengthen California's Next Consumer Data Privacy Initiative

EFF and a coalition of privacy advocates recently asked the sponsor of a new California ballot initiative to strengthen its provisions on consumer data privacy. The California Consumer Privacy Act of 2018 (CCPA) created new ways for the state's residents to protect themselves from corporations that invade their...

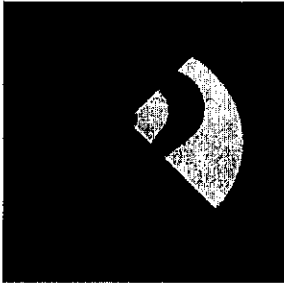


DEEPLINKS BLOG BY HAYLEY TSUKAYAMA | OCTOBER 29, 2019

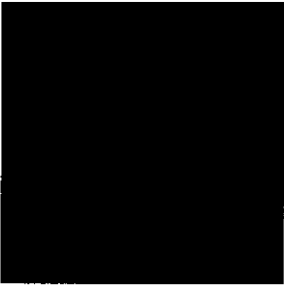
Facebook Faces Another Congressional Grilling

Facebook chief executive Mark Zuckerberg was called back to Capitol Hill to speak about the company's impact on the financial and housing sectors—particularly in light of its proposal to launch a cryptocurrency wallet, Calibra, and its involvement in the creation of the Libra cryptocurrency. We've criticized Facebook on ...

Companies Can Still Do More to Protect Privacy in Brazil: Internet Lab Releases Fourth "Who Defends Your Data" Report



DEEPLINKS BLOG BY VERIDIANA ALIMONTI | OCTOBER 29, 2019
Internet Lab, the Brazilian independent research center, has published their fourth annual report of “Quem Defende Seus Dados?” (“Who defends your data?”), comparing policies of their local Internet Service Providers (ISPs) and how they treat users’ data after receiving government requests. **Vivo (Telefónica)** still takes the lead, but...



DEEPLINKS BLOG BY ERNESTO FALCON | OCTOBER 28, 2019
DNS over HTTPS Will Give You Back Privacy that Big ISPs Fought to Take Away
An absurd thing is happening in the halls of Congress. Major ISPs such as Comcast, AT&T, and Verizon are banging on the doors of legislators to stop the deployment of DNS over HTTPS (DoH), a technology that will give users one of the biggest upgrades to their Internet privacy...



PRESS RELEASE | OCTOBER 22, 2019
EFF and Partners Urge U.S. Lawmakers to Support New DoH Protocol for a More Secure Internet

San Francisco—The Electronic Frontier Foundation (EFF) today called on Congress to support implementation of an Internet protocol that encrypts web traffic, a critical tool that will lead to dramatic improvements in user privacy and help impede the ability of governments to track and censor people. EFF, joined by Consumer Reports and...

EFF Challenges Ring Spokesperson Shaq Over Privacy Concerns



**DEEPLINKS BLOG BY MATTHEW GUARIGLIA, JASON KELLEY |
OCTOBER 21, 2019**

EFF is asking Ring spokesman Shaquille O’Neal to cancel his appearance at a party hosted by the company at the upcoming International Association of Chiefs of Police conference on October 27. Instead, we’re challenging Shaq to a one-on-one: not on the basketball court, but across the table, so we can...

ELECTRONIC FRONTIER FOUNDATION
eff.org
Creative Commons Attribution License



Los Angeles Times

Log In



Case 1:19-cv-03297-TWT

ADVERTISEMENT

BUSINESS

Column: Did the FTC mislead consumers about its Equifax data breach settlement? Yes!



Equifax's reputation isn't glowing. (Justin Lane / EPA)

By MICHAEL HILTZIK
BUSINESS COLUMNIST

SEP. 10, 2019
6 AM



The Federal Trade Commission is supposed to protect consumers from being deceived by businesses. But what happens when the FTC itself is the

deceiver?

That question arises in connection with to with a new wrinkle in the settlement of up to \$700 million that the agency and other regulators reached in July with Equifax, a credit bureau that allowed the personal data of as many as 145 million consumers to be breached by hackers.

Thousands, and perhaps millions, of victims are just now discovering that they'll have to jump through an unexpected hoop if they wish to take advantage of a \$125 settlement payout that's one of the options for compensation.

It appears the agency itself may have misled the American public about the terms of the Equifax settlement and their ability to obtain the full reimbursement to which they are entitled.

SEN. ELIZABETH WARREN, D-MASS.

The discovery has come through an email sent to applicants by the settlement administrators, threatening to deny their applications for the cash payout if they don't respond with some personal information by Oct. 15. The email is sufficiently generic that it might be deleted, whether automatically or by a recipient's choice, as spam. That's what happened to two separate emails sent to my household.

ADVERTISEMENT

The FTC knows the email looks bogus. In a Q&A on its [web page detailing the settlement](#), it acknowledges that consumers might ask: "I got an email about the settlement. Is it legit?" Its answer is "Yes."

Column: Here are all the ways the Equifax data breach is worse than you can imagine

Sep. 8, 2017

This is only the latest bait-and-switch connected with the Equifax settlement, which was announced July 22 and billed as the largest such settlement ever in a data breach case. The settlement covered claims made against Equifax by the FTC, the Consumer Financial Protection Bureau and 50 states and territories. Like many such settlements, a big number ends up amounting to pennies on the dollar for individual victims.

The fine print in the Equifax case began to emerge almost immediately. It transpired that only \$31 million of the total settlement was allocated to the cash payout. As Sen. Elizabeth Warren (D-Mass.) observed in a blistering letter to the FTC, that would cover only 248,000 individuals, or less than 1% of the 145 million consumers affected by the breach.

If more than 248,000 requested the cash, the payout would be reduced on a pro-rata basis. If all 145 million victims requested cash, they'd each receive 21 cents. The rest of the settlement covered civil penalties and the cost of credit monitoring to be offered victims for free.

BUSINESS

Column: LifeLock offers to protect you from the Equifax breach — by selling you services provided by Equifax

Sep. 18, 2017

"It appears the agency itself may have misled the American public about the terms of the Equifax settlement and their ability to obtain the full

reimbursement to which they are entitled,” Warren wrote.

With that in mind, consumer advocates were forced to advise the victims that the alternative compensation — up to 10 years of “free monitoring of your credit report at the three credit bureaus (Equifax, Experian and TransUnion) and \$1,000,000 of identity theft insurance” — might be the better choice.

Among them was Rep. Alexandria Ocasio-Cortez (D-N.Y.), who initially advised constituents to opt for the cash, but then backtracked.

Okay everyone UPDATE on Equifax: for most people the better deal is 10 years of free credit monitoring.

There’s apparently a run on settlements so there’s anxiety people are going to get 16 cent checks. But if you choose 10 years of credit monitoring, Equifax **must** cover it.

— Alexandria Ocasio-Cortez (@AOC) July 27, 2019

The latest wrinkle involves the realization that the \$125 cash benefit was available only to people who already had credit monitoring in place (possible as a benefit from an earlier data breach permitted by our stunningly lackadaisical retailers, banks and data firms.

The FTC says it believes it has given consumers adequate notice of the terms of the deal. “We would dispute the assertion that we had not previously made clear that the alternative cash payment was for those affected consumers who already have credit monitoring,” FTC spokeswoman Juliana Gruenwald told me by email. She cited a [July 22 blog post](#) specifying that “affected consumers were only eligible for the alternative cash option if they already had credit monitoring.”

Gruenwald noted that the FTC, in a July 31 blog post, notified applicants to expect an email from the settlement administrator asking them to identify the credit monitoring service they already have.

Yet the agency's multiple web postings arguably have stoked consumer confusion. The deal, the FTC said in [a July statement](#), was for "up to 10 years of free credit monitoring OR \$125 if you decide **not** to enroll because you already have credit monitoring." What wasn't clear was that you couldn't seek the cash payout *unless* you didn't have credit monitoring already.

BUSINESS

Column: Insurance firms' blunders on long-term care insurance create disaster for millions

July 25, 2019

In yet another notice [posted on its website and dated this month](#), the agency says that the settlement includes free credit monitoring for up to 10 years and adds parenthetically: "(Previously, a cash payment was identified as an alternative to the free credit monitoring, but there are limited funds available.)"

The FTC seems to have decided that most consumers would have no trouble navigating through its multiple formulations of the settlement terms. Bad call, since the FTC itself seems to have been rather confused itself. For an agency with the job of ensuring that people aren't misled or cheated by the fine print in consumer contracts, its failure to make the terms crystal clear up front, and in **BOLD TYPE**, is inexcusable.

The bottom line is that countless Americans signed up for a \$125 cash

benefit plainly on the assumption that they'd get \$125, on the condition only that their data had been breached--which they could determine by plugging their name, address and a few other personal facts into a settlement website. Interestingly, the website currently requires applicants for the cash benefit to give the name of their existing credit monitoring service before proceeding. That's new. As recently as Aug. 3, according to a web archive, claimants who opted for the cash benefit were asked only if they wanted the money paid by check or pre-paid card.

That brings us to the email, which only showed up in my email account on Saturday. The email, which came from the Equifax Breach Settlement Administrator, informs applicants to "verify your claim for alternative compensation by providing "the name of your credit monitoring service that you had in place when you filed your claim."

BUSINESS

Column: If a \$5-billion fine won't shake Facebook, what can bring it to heel?

July 18, 2019

The email warns, "Please note that if you do not take action by October 15, 2019, your claim for alternative compensation will be denied." Applicants can still change their choice to free credit monitoring until the application deadline, next Jan. 22.

This is, of course, an ancient dodge well understood by insurance companies and other consumer-facing businesses: With every hoop claimants are forced to jump through, a certain percentage will give up. That's why the first, reflexive response by a health plan to a big claim is to deny it, forcing the

claimant to file an appeal. Then that's denied, requiring yet another appeal, and after a few months of this roundelay a sizable liability can be whittled away to nothing.

Should the nation's premier consumer watchdog be participating in what is, at heart, a scam? The email doesn't merely present a hoop to jump through, but requires consumers to rummage through their records to find the name of their credit monitoring service and submit proof that the service will remain in force for at least six months after the date they filed their initial claim.

This is a classic example of the proverbial "Hobson's choice" — a choice in which only one thing really is being offered. In other words, no choice at all. Free credit monitoring may be the right choice for many of Equifax's victims, or it might not. Quite a few victims might reasonably wonder at the value of a service being offered by the very firm that created their problem in the first place, through an inexcusably lax approach to the security of the personal data of half the residents of the United States.

Yes, the credit monitoring might be free, but it might be worth nothing. But forget about the \$125 alternative--it doesn't really exist in the real world.

The Equifax settlement is beginning to look not like a triumph of regulatory scrutiny, but just another ripoff--but government certified.

BUSINESS

NEWSLETTER

Get our weekly California Inc. newsletter

Please enter your email address

Subscribe



Michael Hiltzik

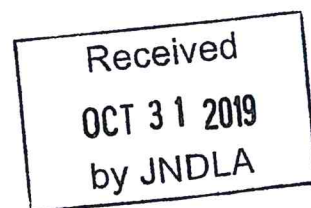
- Twitter
- Instagram
- Email
- Facebook

Pulitzer Prize-winning journalist Michael Hiltzik writes a daily blog appearing on latimes.com. His business column appears in print every Sunday, and occasionally on other days. As a member of the Los Angeles Times staff, he has been a financial and technology writer and a foreign correspondent. He is the author of six books, including “Dealers of Lightning: Xerox PARC and the Dawn of the Computer Age” and “The New Deal: A Modern History.” Hiltzik and colleague Chuck Philips shared the 1999 Pulitzer Prize for articles exposing corruption in the entertainment industry.

MORE FROM THE LOS ANGELES TIMES

CALIFORNIA
Sweeping bill on independent contractors passes California state Senate
Sep. 10, 2019

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418



Dear Sir or Madam,

I am writing *In re: Equifax Inc. Customer Data Security Breach Litigation*, Case No. 1:17-md-2800-TWT, the "Equifax Data Breach Lawsuit"

I found my name in a database as someone who was affected by the breach and was given the option to request compensation. I requested the \$125 compensation. Then I got an email that unless I had put credit monitoring in place as a result of the breach and could prove it, I would not receive any compensation. I think this is very wrong. The total compensation to those affected was minimal and my exposure to my credit being affected is ongoing. If I do have a problem, there will likely be no money left by the time it happens. I spent a considerable amount of time weighing my options and decided the credit monitoring wasn't worth the cost. If I knew I would be compensated (although the compensation appears to be inadequate), I would have made a different calculation. And here I am now spending more time writing a letter to object.

Apparently all the risk as well as the work of trying to receive compensation goes to the victims. This is not right.

Also, Equifax should have covered all expenses. The small settlement they were asked to pay is hardly a deterrent and I expect there to be breaches in the databases in the future. If all they have to do is pay a relatively small fine, they will have little incentive to fix the problem and have adequate security in their systems.

This whole process has been extremely disheartening. You should be working to improve Americans trust in government oversight. This ruling has significantly undermined it.

I have not objected to any class action settlements in the past 5 years.

I will not be at the Fairness Hearing and I don't have a lawyer.

Sincerely,

A handwritten signature in black ink, appearing to read "Jennifer Hart".

Jennifer Hart

1451 East 55th St. 717N

Chicago, IL 60615

UNIVERSITY OF CHICAGO LIBRARY
ECKHART LIBRARY
1118 EAST 58TH STREET
CHICAGO ILLINOIS 60637-1338

Jenny Hunt

1451 E 55TH ST 717N
CHICAGO, IL 60615

OCT 31 2019

Equifax Data Breach Class Action
Attn: Objection
C/O JND Legal Administration

PERMIT NO. 19
378.98111-9418
SEATTLE, WA



SUBSCRIPTION II 604

28 OCT 2019 PM 5:1



JILL ANNE GAMBARO

Oct. 18, 2019

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418



In re: Equifax Inc. Customer Data Security Breach Litigation
Case No. 1:17-md-2800-TWT
"Equifax Data Breach Lawsuit"

Your Honor,

I am writing to object to the settlement in the above-referenced legal action. I am a member of the settlement class, as is pretty much anyone in the United States with a social security number. I did not choose Equifax to be the holder of my personal data, as few of us have. I did not provide Equifax with any of my data; they collected it of their own accord. I do not recall giving them any permission to do so; if I did, it was by force, not by choice. I was never informed that Equifax was selling my information to third parties. They never sought my permission. I never gave them permission to sell my information to potential employers. I was never paid by Equifax for collection my information.

I object to the settlement on the grounds that it's insufficient an amount to adequately compensate every one whose data Equifax holds. Simply offering free credit monitoring services is neither punishment for Equifax, nor an adequate remedy for those of us who's information has been stolen. I am the victim of no less than three such data breaches by large companies over the past several years alone. I already have free credit monitoring services twice over. My guess is so do a lot of other people. Additionally, this doesn't cost the company very much at all does it? Furthermore, that there may not be adequate funds to cover everyone who's seeking monetary compensation tells me the final figure is not big enough, not that those of us who are victims of this crime should do with less. Finally, the entire business model upon which Equifax works in violation of anti-trust laws.

I have never objected to any other class action settlement. I do not intend to appear at the Fairness Hearing, though I am available for deposition on November 19, 20, 21, and 22, 2019 to be deposed by counsel for the parties.

Sincerely,

A handwritten signature in cursive script that reads "Jill Gambaro".
Jill Gambaro

SANTA CLARITA, CA 913

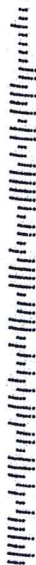
19 OCT 2019 PM 5 L

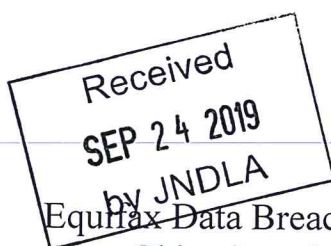


OCT 23 2019

Equifax Data Breach
Class Action Settle Admin
Attn: Objection
c/o JND Legal Admin
P.O. Box 91318
Seattle WA 98111-9418

98111-9418





September 20, 2019

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

In re: Equifax Inc. Customer Data Security Breach Litigation,
Case No. 1:17-md-2800-TWT

Full Name and Current Address: Jill W. Mansfield, 628 Ravenwoods Dr.,
Chesapeake, VA 23322

Personal Signature: 

I feel that I am a member of the settlement class. I checked the Equifax online site and it indicates that I am an effected customer/member of the settlement class. I filed an online claim on July 26, 2019. My claim number is PNLHQ-Y3TRK

I feel deceived by the terms of the cash payout for those of us who already have credit monitoring services in that we will receive only pennies on the dollar amount of the claim. I updated my claim online earlier today to indicate that their fraud department monitors my existing ABNB FCU cards.

I have not objected to any class action settlements within the past 5 years.

I do not intend to appear at the Fairness Hearing.

Sincerely,

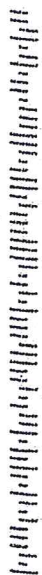
Jill W. Mansfield

Mark Mansfield
628 Ravenwood Dr.
Chesapeake VA 23322

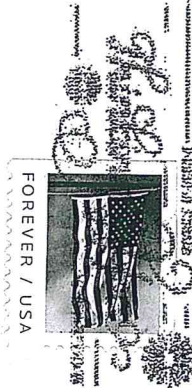
SEP 24 2019

Enifax Data Breach Class Action Settlement Admin.
Attn: Objection c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

98111-941818

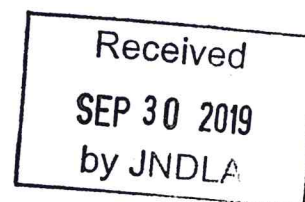


RICHMOND VA 230
21 SEP 2019 PM 21



Harrison Andrew Neal
7902 Bubbling Brook Cir
Springfield, VA 22153

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418



OBJECTION TO PROPOSED SETTLEMENT
In re: Equifax Inc. Customer Data Security Breach Litigation
Case No. 1:17-md-2800-TWT

Required Information.

My name is Harrison Andrew Neal, currently residing at 7902 Bubbling Brook Circle, Springfield, VA, 22153.

I am a member of the settlement class according to the settlement website, which prompted me to confirm personal details (i.e., last name, several digits of my social security number, etc.) prior to informing me of my status and allowing me to file a claim.

I do not recall objecting to any class settlements in the past 5 years.

At this time, I do not believe I am able to attend the fairness hearing due to schedule conflicts. If that changes prior to the submission deadline of November 19th, 2019, I will send clarifying correspondence as soon as possible.

Rationale for Objection.

The proposed settlement would offer “at least” 4 years of credit monitoring through Experian, followed by “up to” 6 years of credit monitoring through Equifax ¹.

Entities that have experienced data breaches have previously attempted to placate affected individuals with offers of free credit/identity monitoring, insurance, or similar services, either as a proactive step ² or as part of a settlement ³. The federal government

A handwritten signature in dark ink, appearing to be "HAN" or similar, written over a horizontal line.

¹ <https://www.equifaxbreachsettlement.com/>

² <https://www.delta.com/us/en/advisories/other-alerts/response>

³ <https://www.nbcnews.com/tech/tech-news/yahoo-pay-50m-offer-credit-monitoring-massive-security-breach-n923531>

is also familiar with this unfortunate routine, having offered various services to over 20 million people ⁴ , including myself, following the OPM data breach.


Data breaches, and subsequent offers of protection, have unfortunately become very common around the world. In recent years, billions of records have been affected by data breaches ⁵ . Credit/identity reporting and monitoring entities have explicitly marketed services to other entities concerned about handling data breaches ⁶ ⁷ .

Between the number of entities already offering credit/identity monitoring or insurance as a result of other data breaches, and various credit/identity monitoring tools that are free of charge ⁸ or included with various financial products ⁹ , the offer of such services is likely redundant if not meaningless for many individuals affected in this data breach.

Unfortunately, the structure of the proposed settlement suggests that its authors have failed to grasp that offering affected individuals something they already have is not appropriate restitution, and certainly should not be considered the primary means of restitution. Recent blog posts by the FTC ¹⁰ suggest this wrong-headed thinking persists.

Even if the nature of the services offered through the proposed settlement were acceptable, the length of time offered is inadequate. Individuals impacted by data breaches could experience future harm long after “complimentary” services end ¹¹ , and this proposed settlement only offers services for an advertised total of 10 years.

Americans currently have a life expectancy of 80 years, and 84% of Americans are less than 65 years old ¹² . If the overall demographic of this country is comparable to the demographic of individuals impacted by the Equifax data breach, the overwhelming majority of affected individuals would be expected to outlive offered services, even if those services lasted the advertised 10 years.


⁴ <https://www.opm.gov/cybersecurity/>

⁵ <https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002/>

⁶ <https://www.experian.com/data-breach/data-breach-solutions.html>

⁷ <https://www.transunion.com/solution/data-breach-services>

⁸ <https://www.creditkarma.com/>

⁹ <https://www.discover.com/credit-cards/member-benefits/security/ssn-newaccount-alerts/>

¹⁰ <https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-pick-free-credit-monitoring>

¹¹ <https://www.afge.org/globalassets/documents/data-breach/cardin-letter-data-breach.pdf>

¹² https://en.wikipedia.org/wiki/Demography_of_the_United_States

While the proposed settlement supposedly offered an alternative to all affected individuals in the form of a cash payment, the funding for individuals choosing this option is woefully inadequate, so much so that at least one US Senator has requested that the FTC's inspector general investigate if the FTC's original announcement was misleading to the consumers they were ostensibly fighting on behalf of ¹³. If this lack of funding is not addressed, the proposed alternative would offer a pittance.

Somewhat ironically, at the time of writing, one of the web pages concerning this case ¹⁴ on the FTC's website displayed a large button labeled "file a claim" with a dollar symbol, and the breadcrumbs in the page's header included the word "refunds", both of which could be construed as continuing to mislead affected individuals.

Put simply, for those that already have monitoring or insurance services, the choice between a service one already has and a negligible amount of money is unfair. For all others, there is a strong likelihood that they, along with the risks to their identities, will outlive the offered services, which is also unfair.

Finally, considering that Equifax was negligent with regards to computer security ¹⁵ after various other entities experienced data breaches and offered affected individuals "remedies" ¹⁶ similar to those being proposed in this case, a reasonable person may conclude that the cost of those "remedies" was and remains inadequate for deterring future negligence. Affected individuals will never be made whole if their sensitive information is breached from third parties on a regular basis, and entities that lose such information should be subject to damages and/or penalties that are adequate to deter future negligence.

In conclusion, the proposed settlement is inadequate in a number of ways, will fail to provide meaningful restitution to affected individuals, and will continue an overused precedent that loses value with each additional data breach.

Harrison Neal
27 September 2019

x  27 Sep 2019

¹³

<https://www.warren.senate.gov/imo/media/doc/2019.08.13%20Letter%20to%20FTC%20IG%20on%20Equifax%20settlement.pdf>

¹⁴ <https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement>

¹⁵ <https://techbeacon.com/security/why-equifax-breach-should-never-have-happened>

¹⁶ <https://www.marketwatch.com/story/free-credit-monitoring-after-data-breaches-is-more-sucker-than-succor-2015-06-10>

WILKINSON NEAL
7902 BUBBLING BROOK CIR
SPRINGFIELD, VA 22153

NOVA 220
27 SEP 2019
PM 2L



1000



98111

U.S. POSTAGE PAID
FCM LETTER
ALEXANDRIA, VA
22312
SEP 27, 19
AMOUNT

\$6.85

R2305H157817-67

PLACE STICKER AT TOP OF ENVELOPE TO THE RIGHT
OF THE RETURN ADDRESS, FOLD AT DOTTED LINE

CERTIFIED MAIL®

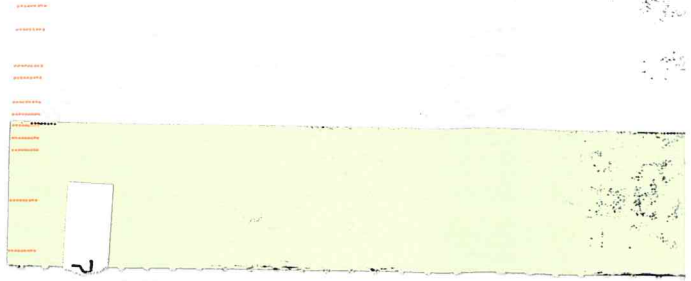
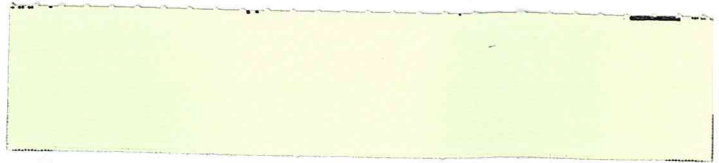


7018 0360 0001 4126 5105

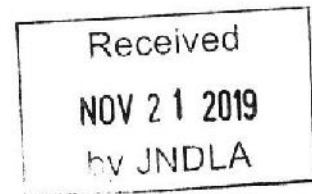
Equifax Data Breach Class
Action Settlement Administrator
Attn: Objection
% JND Legal Administration
PO Box 91318
Seattle, WA 98111-9418

SEP 30 2019

98111-941818



Heidi Struse
908 Princeton Dr SE
Albuquerque, NM 87016



Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

To whom it may concern:

I am writing to inform the Court about my objection to certain terms and conditions of the proposed Equifax settlement. The underlying litigation is identified as *In re: Equifax Inc. Customer Data Security Breach Litigation*, Case No. 1:17-md-2800-TWT. I believe I am a member of this settlement class, because I was informed of same by visiting the data breach website and entering my Social Security number.

Specifically, the course of action that I chose following this breach was to freeze my credit with all three reporting agencies, which is a cumbersome, onerous and annoying procedure, as I have to lift these freezes in the event that I wish to be reinstated to the practice of law in New Mexico, for example. But the proposed Equifax settlement mandates that I choose credit monitoring, which is something I do not wish to do. Why would any credit monitoring service be any more trustworthy than Equifax was to begin with? Even a freeze is not perfect, but I believe for me it offers better protection than any monitoring service.

It is one thing for Equifax to propose to offer some nugatory compensation to persons affected by their data breach. But it is unreasonable and unfair for Equifax to dictate the terms of this paltry payout, and it seems a blatant and transparent attempt to avoid making such payouts, as many people will not sign up for credit monitoring.

I have not objected to any class action settlements ever, but this article in the New York Times, <https://www.nytimes.com/2019/09/16/opinion/equifax-settlement.html>, made me realize that this time I wanted to weigh in.

I do not intend to appear at the Fairness Hearing.

Sincerely,

A handwritten signature in dark ink, appearing to read "Heidi Struse".

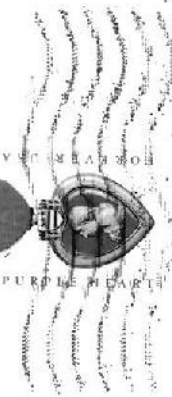
Heidi Struse

Held Struse
908 Princeton Dr SE
Albuquerque, NM 87106

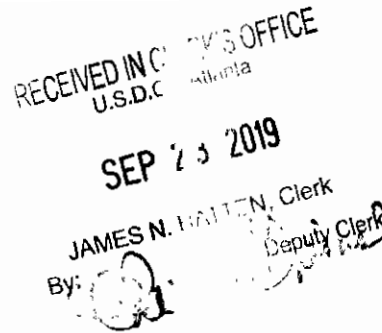
NOV 21 2019

Equifax Data Breach Class
Action Settlement Administrator
Attn = Objection
c/o INS legal Administration
P.O. Box 91318
98114
98114-1318

U.S. MAIL PERMIT NO. 1000
ALBUQUERQUE, NM 87106



US District Court for the Northern District of Georgia
75 Ted Turner Dr NW Ste 2211
Atlanta GA 30303



RE: Equifax Data Breach Settlement Procedure

I am writing to object to the way the Equifax data breach settlement procedure is being handled. As a credit bureau, Equifax holds the complete financial information for nearly every adult citizen in the country. There is immense power in this data and an immense requirement to protect it. Equifax did not secure this information properly and as a result caused real damage to millions of people who have had to take steps to protect themselves. A settlement was reached intended to compensate consumers and a public announcement was made that \$125 would be available to affected consumers who applied.

Since the announcement and application process were made public, the situation has been a mess, with not enough funds set aside to pay actual claims and confusing roadblocks placed in the way of consumers. First, everyone was encouraged to take the free credit monitoring, which of course costs Equifax nothing. However, most people already have free credit monitoring from another data breach or through their credit cards or financial institution and most people know this. Because of this, too many people put in a claim for the cash so a confusing, spammy email was sent in the middle of a weekend, giving people a deadline by which they had to **prove** they had credit monitoring, the obvious purpose of which was to keep people with legitimate claims from receiving the money they were promised. In addition to the fact that the email did not seem legitimate and in some cases wound up in spam folders, no guidance about what was acceptable "proof" was given. There was a free-form line to complete and that's it. I have worked in banking for 28 years and have credit monitoring through 2 credit cards and my primary credit union. I wrote in "UW Credit Union CreditView through TransUnion." I have no idea if this is sufficient, though it is true, accurate, ongoing credit monitoring and should be valid as proof. As someone with years of experience in finance, this was confusing to me. Others with no experience are going to miss the email altogether, not understand it, or if they do understand it, aren't going to have the vaguest idea what to write. This is shameful, enraging, and should be embarrassing for those behind it.

A handwritten signature in black ink, appearing to read "Heidi Wilhelm", with a long, sweeping horizontal line extending to the right.

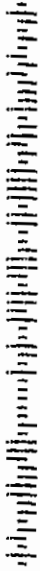
Heidi Wilhelm
1525 Longview St.
Madison WI 53704

ATTENTION
WI 532
20 SEP '19
FN 7 L

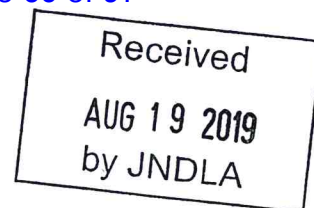


US District Court the W. District of GA
75 Ted Turner Dr. NW Ste 2011
Atlanta GA 30303
Re: Equifax Breach Settlement

30303-331861



Ms. Heidi Wilhelm
1525 Longview St.
Madison, WI 53704



August 13, 2019

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

In re: Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT

I wish to object to the aforementioned settlement. I confirmed that my personal information was compromised by entering my information on the following website <https://eligibility.equifaxbreachsettlement.com/en/eligibility>. I have not received any notices regarding the breach via mail. I have not obtained an attorney for this objection and I have not objected to any class action settlements within the past 5 years. I will not be attending the fairness hearing for the objection.

Below are my objections and reasons:

I am troubled that the credit monitoring wasn't automatically extended to all persons with credit records at Equifax, rather than making this an "opt-in" consumer-driven benefit long after the breach.

While the first 4 years of the 10-years credit monitoring term may have a retail price of \$30/month, did anyone consider that the cost to Equifax for this service is nearly nothing (as everything is done by computer with no human intervention)? I think that Equifax, given the gravity of the breach, should be forced to pay the attorney fees directly and not out of the fund established for consumer restitution. This would send an even stronger message to Equifax and other companies who aren't doing enough to protect our data.

It seems that credit reporting businesses are focused more on their revenue and "monetizing the data," rather than making sure their data is accurate and secure. Consumers never had a choice to be Equifax's customer. When data is breached, it is breached for life. The terms of this settlement are completely unacceptable. I have had credit monitoring and ID theft services since 2014, however, my data has been compromised. This settlement does not hold Equifax accountable for lifetime harm, which is inevitable, nor does it provide individual victims a way to identify exactly what data was stolen. Frankly, the credit monitoring offer or an unknown cash amount offer due to millions of people being compromised does not equate to damages that will occur in the long term.

Regards,

Helen A. Coxhead

A handwritten signature in black ink that reads "Helen A. Coxhead". The signature is fluid and cursive, with a long horizontal line extending from the end.

137 Midway Island
Clearwater FL 33767

C Helen Coxhead
137 Midway Is.
Clearwater Beach, FL 33767

TAMPA, FL 335
SAINT PETERSBURG FL
15 AUG 2019 PM 4 L



Equifax Data Breach Class Action Settlement Administration
Attn: OBSection
c/o JND Legal Administration
PO Box 91318
Seattle WA 98111-9418

98111-9418



Hilary G. Escajeda

743 Syracuse Street
Denver, CO 80230

September 23, 2019

Honorable Thomas W. Thrash, Jr.
Richard B. Russell Federal Building
United States Courthouse
75 Ted Turner Dr., SW
Atlanta, GA 30303-3309

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

Re: Objection to credit monitoring, cash payment requested
In re: Equifax Inc. Customer Data Security Breach Litigation
Case No. 1:17-md-2800-TWT

Dear Judge Thrash and Class Action Settlement Administrator:

I write to object to the Equifax Data Breach Settlement, which has now taken the form of credit monitoring rather than cash payment.

I request payment in cash for two reasons. First, because my name was included on the Equifax breach list, I implemented a credit freeze. Credit monitoring is, therefore, unnecessary since I have the highest level of identity theft protection. The credit freeze provides ample security since it requires several steps to complete a simple task such as switching cell phone carriers.

Second, and most importantly, I feel deceived by the settlement process. Specifically, Equifax offered monetary compensation for the breach. I submitted a claim according to their process. Since I followed the settlement claim process and accepted their offer of cash compensation, I expect that they abide by the original terms of the settlement. Shifting the terms of a settlement after relying on their earlier representations and claim submission process reinforces the impression that well-funded corporations can renege on their promises and act with impunity toward ordinary citizens without teams of lawyers advocating for their legal rights. This Court has the authority to ensure the fair and reasonable treatment of all class members harmed by Equifax's failure to protect sensitive financial information.

To the best of my knowledge, I have not previously objected to any class action settlement in the past five years. Since I live in Colorado, I will not attend the hearing in Atlanta on December 19, 2019.

I request that the Court order that Equifax pays all class members the monetary award per their original offer. Thank you for considering my objection.

Sincerely,



Received
SEP 26 2019
by JNDLA

743 Syracuse Street
Denver, CO 80230

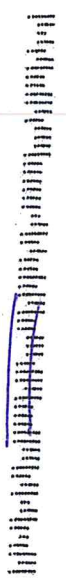
DENVER CO 802
23 SEP 2019 PM 11



Equity Rate Break Class Action Settlement Adm.
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418
SEP 26 2019

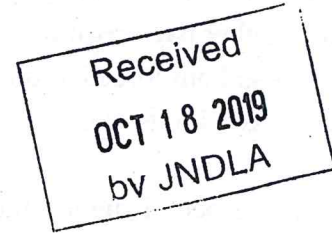
ATTN: Objections

9011-9418



Ian Korn
1089 Eastern Parkway
Apt. 16D
Brooklyn, NY 11213

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418



In re: Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT

To the Honorable Members of the Court:

I write in objection to the aforementioned settlement, as it is very clearly inadequate to sufficiently compensate all of those affected.

According to Equifax's online look-up tool (located at <https://eligibility.equifaxbreachsettlement.com/en/eligibility>), I am a member of the class, as my personal data was exposed in the data breach.

As has been widely reported, if all 147 million members of the affected class were to claim monetary compensation under this settlement, we each would receive only \$0.21. Even if half of us did, that's still under a dollar as compensation for the potential of our lives being completely upended by our personal data being exposed.

The offer of free credit monitoring from Equifax as an alternative is absurd. The company's single job is to monitor, report on, and *safeguard* consumers' personal credit history and information, and it has demonstrated it cannot be trusted to perform that duty. I cannot put any faith in Equifax to allow them to be my primary credit monitor. Furthermore, free credit monitoring of some sort is offered by most credit card companies. I personally have some form of monitoring from at least three credit cards and one budgeting service, in addition to the federally-mandated annual free credit report.

It should also be added that the cash compensation offered would not begin to cover credit monitoring services from a third party, which range from \$10-\$20 a month, and would be required for the rest of my lifetime thanks to Equifax's failures.

The thing that makes this settlement most objectionable, though, is that at no time was I, a consumer with a credit history, ever given a real choice as to whether or not to use Equifax's services. By the simple act of opening a credit card, taking out a student loan, considering a loan for anything else, investigating a mortgage, etc., my personal information is passed on to Equifax and the other two credit bureaus. Of course, I don't really have an option not to do any of those things - so I am forced to rely on Equifax, a private company with a monopoly that has shown it is careless with its work.

With all respect, I suggest the court object to this settlement as thoroughly inadequate.

I have never before objected to a class action settlement I have been a class member of.

I do not intend to appear at the scheduled Fairness Hearing, and trust that the Honorable Court will do what is right.

Thank you for your consideration.

Sincerely,



Ian Korn



Ian Daniel Korn
1089 Eastern Pkwy Apt 16D
Brooklyn, NY 11213

OCT 18 2019

EAUFAA Data Breach Class Action Administrator
ATTN: OBJECTION
C/O IND LEGAL ADMINISTRATION
P.O. Box 91318
SEATTLE, WA 98111-9418

98111-9418



NEW YORK NY 100

19 OCT 2019 PM 6:19



J. Peter Wyke
101 Shogbuck Lane
Williston, VT 05495

Oct 17, 2019

Equifax Data Breach class Action Settlement Administration

Attn: Objection

c/o JND Legal Administration

PO Box 91318

Seattle, WA 98111-9448

Received

OCT 22 2019

by JNDLA

Dear Sir or Madam.

I object to the proposed settlement

I have been identified as a member of the settlement class as a result of clicking the appropriate box furnished by Equifax and entering my last name and last 6 digits of my social security #. in the matter of the Equifax Data Breach lawsuit.

my objection is that the total amount of the settlement is insufficient to pay the proposed amount to all of those affected by the data breach as reported in the media

I have not objected to any class action settlements in the past 5 years.

I do not intend to appear at the Fairness Hearing either in person or through counsel.

Sincerely

J. Peter Wyke

BURLINGTON VT 054

18 OCT 2019 PM 1 L



JOHN JUDGE
101 SHAGBARK LANE
WILLISTON, VT 05495

OCT 22 2019

Equifax Data Breach class Action
Settlement Administrator

Attn: objection

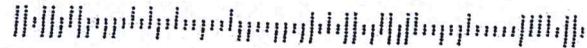
c/o JND Legal Administration

PO Box 91318

Seattle, WA 98111-9418

Received
OCT 22 2019
by JNDLA

98111+9418



JACK L SMITH

4779 W Pier Mountain Pl., Marana, AZ 85658

10 October 2019

Attn: Objection

Equifax Data Breach Class Action Settlement Administrator
% JND Legal Administration
PO Box 91318
Seattle, WA 98111-9418

In re. Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT

Gentlemen:

I object to the proposed settlement because the amount of the settlement allocated to individual class members is NOT SUFFICIENT. In view of the likely number of members of the class, the settlement provides no meaningful compensation.

I have tested my particulars using <https://www.equifaxbreachsettlement.com> and was informed that I am included in the class.

I have not objected to any class action settlements in the previous five years and do not intend to appear at the Fairness Hearing.

Jack L. Smith
4779 W Pier Mountain Pl
Marana, AZ 85658,



Jack L. Smith

Received
OCT 15 2019
by JNDLA

JACK L SMITH
4779 W Pier Mountain Pl, Marana, AZ
85658

PHOENIX, AZ 850

10 OCT 2019 PM 4:11



Equifax Data Breach Class Action Settlement Administrator
Attn: Objection

% JND Legal Administration

PO Box 91318

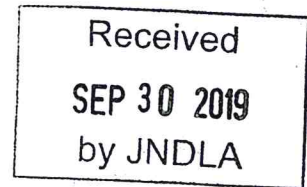
Seattle, WA 98111-9418

OCT 15 2019

98111-9418



Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418



In re: Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT

We are members of the settlement class. We received letters from Equifax stating we are.

The settlement offers 10 years of credit monitoring or a \$250 settlement. Since we already have credit monitoring, we chose the settlement. Subsequently, we filed statements with them stating we already have credit monitoring through Lifelock. All of this was done electronically on the settlement website.

Apparently, if all of the millions of us affected by their data breach file for the \$250 settlement, we will all receive 21¢ (that is not a typo, that is twenty one cents). This is a slap on the wrist for Equifax and an insult to those of us affected by their breach.

We have not objected to any class settlements in the past five (5) years.

We do not intend to appear at the Fairness Hearing, either in person or through a lawyer. 21¢ each will not compensate us for the cost of doing so.

A handwritten signature in cursive script, appearing to read "Milton D. Weedon, Jr.".

Milton D. Weedon, Jr.

A handwritten signature in cursive script, appearing to read "Jacquelyn Ann Weedon".

Jacquelyn Ann Weedon

336 Woody Circle
Tryon, NC 28782

September 25, 2019



SEP 30 2019

[illegible]

1136 South Washington Street #103
Falls Church, VA 22046-4027
3 October 2019

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

Received
OCT 08 2019
by JNDLA

Dear Administrator and Judge Thrash:

I write to state my strident objection to the Equifax Breach Settlement (*In re: Equifax Inc. Consumer Data Security Breach Litigation*, Case No. 1:17-md-2800-TWT).

My name is James C. Benton, and I reside at 1136 South Washington Street #103, Falls Church, VA 22046-4027. I am a member of the settlement class in this case, having been verified through the settlement website established by the claims administrator.

I have not objected to any class action settlements in the past five years. Also, I do not intend to appear at the Fairness Hearing. However, I wish these comments to be entered into the record at the hearing.

This "settlement" is a bait and switch crafted by the administrator, the FTC, and the parties in the lawsuit. You collectively have failed to deliver justice in this case, much less relief to me and the estimated 147 million people who could be part of the settlement class. This is at least the second major data breach I have been affected by in recent years. I resent the offer of "free credit monitoring" offered as part of this "settlement" while attorneys stand to make tens of millions of dollars and Equifax gets off relatively scot-free.

The FTC promised "up to \$125" as an option, but the "settlement" underfunded the amount for consumers who chose that option. Then, after verifying I was a member of the settlement class and opting for the cash payment, the FTC urged everyone to choose the credit monitoring.

To add insult to injury, the administrator sends out an email placing more hoops in our way to jump through at the risk of being excluded from the settlement class.

What is this?

This "settlement" is not justice. This "settlement" is a reflection of why American faith in public institutions has been declining since Watergate. This "settlement" is why many everyday Americans like myself now believe we will never get a fair shake in

dealing with our civic institutions, or that the game is rigged in behalf of the wealthy and powerful.

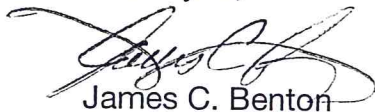
It is absolutely risible that you collectively approve an agreement deliberately underfunding the cash compensation to consumers and offering consumers "credit protection" that for some will fail to reverse the damage they have suffered from the data breach. This bait and switch lets Equifax get away with the bad consequences of this particular data breach without meaningful punishment for their wrongdoing.

I work hard to keep my credit reports accurate and maintain good credit scores. I'd like to believe Equifax cares just as much about my information as I do, but I don't think that's the case. With this bait and switch, the attorneys get paid, Equifax misses any significant penalties for letting my information fall into the wrong hands, and we – the people who have been affected, who may have lost jobs or houses or consumer credit based on this breach – get steered to "free credit monitoring" or out of the settlement class altogether by highly questionable and dishonorable means.

I OBJECT.

I urge Judge Thrash to reject this settlement and direct the parties to negotiate a better settlement that puts affected consumers first. Not the lawyers, not Equifax, but the people who have been hurt by this data breach. You all should be ashamed for structuring this "settlement" in a way that fails to help consumers. DO BETTER.

Thank you,

A handwritten signature in black ink, appearing to read "James C. Benton", is written over a horizontal line.

Cc: Mark R. Herring, Attorney General, Commonwealth of Virginia

1136 SOUTH WASHINGTON STREET #103
FALLS CHURCH VA 22046-4027

NOVA 220

5 OCT 2019 PM 6 L



936490302151611



FOREVER

EQUIFAX DATA BREACH CLASS ACTION
SETTLEMENT ADMINISTRATOR
C/O JND LEGAL ADMINISTRATION
P.O. Box 91318
SEATTLE, WA 98111-9418

OCT 08 2019

50111-941818



Equifax Data Breach Settlement
Action Settlement Administrator
ATTN: Objection
c/o JND Legal Administrator
PO Box 91318
Seattle, WA 98111-9418

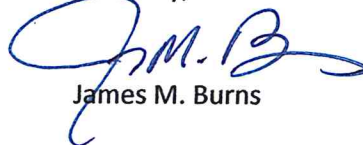
James M. Burns
700 Glenloch Road
Roopville, GA 30170

October 9, 2019

Subject: Objection to Equifax Data Breach Settlement, Per Email September 9, 2019

1. In Re Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT
2. Name of objector: James Michael Burns. Address: 700 Glenloch Road, Roopville, GA 30170
3. I am a member of the settlement class. Per instruction from email dated September 9, 2019 from the Equifax Breach Settlement Administrator, I checked my eligibility. Equifax reports that my personal information was compromised during the breach.
4. I object to the settlement. This settlement is hardly satisfactory and overlooks a class of Equifax customer, like me, who paid Equifax for services which the company did not provide. From 2011-2018, I paid Equifax \$149.95 annually for Equifax ID Patrol, a service which promised to protect my data (see Enclosure 1). I believe that the company owes me \$1,179.60. It failed to protect my information and then failed to inform me, along with thousands of others. I cancelled my subscription to the company's service and even froze my credit, for which it charged me. Evidently, it continues to pretend to monitor my information (see Enclosure 2) in the hopes that I might prove gullible enough to trust it. Or, that it might forestall future litigation. Offering me \$125, maybe, or free credit monitoring through a competitor (Experian) with whom I have frozen my credit is hardly adequate. The settlement is insulting beyond measure and I ask that the court reject it.
5. I have not objected to previous class action lawsuit settlements nor have I made claims that might have benefited me from such a settlement.
6. I would like to attend the Fairness Hearing of December 19, 2019, as I reside within 75 miles of the court. I will make myself available for deposition on one of the following dates: November 20 or 21; December 2 or 3.
7. I am accessible at the physical address above, via email at james.m.burns1@gmail.com or telephonically at 770-542-9026.

Sincerely,



James M. Burns

Received OCT 15 2019 by JNDLA

Enclosure 1 To Equifax Data Breach Settlement - Buens

Profile

For additional assistance contact customer service at 1-877-47GUARD(1-877-474-8273). View our [Terms of Use](#)

Me	Alert Preferences	Manage Billing	Order History	Billing History	Report Manager
Bill Date	Billing Period	Status	Total Charge	Card Details	Payment
03/09/2018	01/09/18 - 01/09/19	Complete	REFUND (\$24.96)	VISA ****-*****-1482	Details
01/09/2018	01/09/18 - 01/09/19	Complete	\$29.95	VISA ****-*****-1482	Details
03/19/2017	03/19/17 - 03/19/18	Complete	\$149.95	VISA ****-*****-1482	Details
01/09/2017	01/09/17 - 01/09/18	Complete	\$29.95	VISA ****-*****-1482	Details
03/19/2016	03/19/16 - 03/19/17	Complete	\$149.95	VISA ****-*****-1482	Details
01/09/2016	01/09/16 - 01/09/17	Complete	\$29.95	VISA ****-*****-1482	Details
01/09/2016	01/09/16 - 01/09/17	Complete	\$29.95	VISA ****-*****-1482	Details
03/19/2015	03/19/15 - 03/19/16	Complete	\$149.95	VISA ****-*****-1482	Details
01/09/2015	01/09/15 - 01/09/16	Complete	\$29.95	VISA ****-*****-1482	Details
01/09/2015	01/09/15 - 01/09/16	Complete	\$29.95	VISA ****-*****-1482	Details
03/19/2014	03/19/14 - 03/19/15	Complete	\$149.95	VISA ****-*****-1482	Details
03/19/2013	03/19/13 - 03/19/14	Complete	\$149.95	VISA ****-*****-1482	Details
03/19/2012	03/19/12 - 03/19/13	Complete	\$149.95	VISA ****-*****-1482	Details

* 03/19/2011 03/19/11 - 03/19/12

\$129.95

©2019 Equifax, Inc., All rights reserved [Online Privacy Policy](#) [Privacy Notice](#) [Terms of Use](#) [FCRA Summary of Rights](#) [Ad Choices](#)

Equifax and the Equifax marks used herein are registered trademarks of Equifax, Inc. Other product and company names mentioned herein are the property of their respective owners.



* The record does not include my first year, which began in 2011. The price that year was \$129.95.

Enclosure 2 To Equifax DATA Breach Settlement - Burns

Profile

For additional assistance contact customer service at
1-877-47GUARD(1-877-474-8273). View our [Terms of Use](#)

Me[Alert Preferences](#)[Manage Billing](#)[Order History](#)[Billing History](#)[Report Manager](#)**Name****James Burns** Account Holder**Current Status**Active[Edit Profile](#)

©2019 Equifax, Inc., All rights reserved [Online Privacy Policy](#) [Privacy Notice](#) [Terms of Use](#) [FCRA Summary of Rights](#) [Ad Choices](#)

Equifax and the Equifax marks used herein are registered trademarks of Equifax, Inc. Other product and company names mentioned herein are the property of their respective owners.



ATLANTA METRO 300

10 OCT 2019 PM 13 L



Equifax Data Breach Settlement
Action Settlement Administrator
ATTN: OBJECTION
c/o JND Legal Administrator
P.O. Box 91318
Seattle, WA 98111-7418

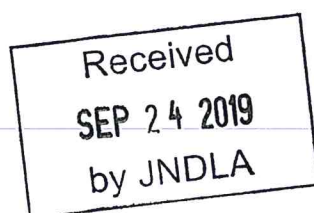
OCT 15 2019

96111-941818



400 Glenloch Rd
Koopeville, GA 30170

James K. Carrow
1479 N. Larrabee St.
Unit A
Chicago, IL 60610



September 17th, 2019

Honorable Thomas W. Thrash Jr.
United States District Court – Northern District of Georgia
Richard B. Russell Federal Building and US Courthouse
75 Ted Turner Dr.
Atlanta, GA 30303-3309

Re: Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT

To the Honorable Thomas W. Thrash Jr. and JND Legal Administration,

My name is James Carrow, and I am writing to you to object to the current settlement terms for the Equifax lawsuit with the Federal Trade Commission. As one of the 147 million people affected by the breach of personal information under the control of Equifax, I continue to feel vulnerable and misled by those involved as it has been well documented that the current funds set aside for compensation are expected to be significantly below the original expressed value (i.e. \$125). I apologize for the brief amount of math: From the \$31 million set aside for victims, an individual would receive \$125 only if ~0.17% of people affected (248,000 out of ~147 million) could have an accepted claim. Less than 1%. Even current U.S. Senators have characterized the handling of this process as “misleading.” This gross misrepresentation of a financial outcome only reduces an already waning public trust in institutions designed to secure our highly sensitive personal and financial information. Further, the Equifax settlement team continues to place hurdles in front of victims to even receive monetary compensation, as demonstrated by the recent email to instructing victims to confirm their monitoring service prior to October 15th.

While I may not be able to provide evidence from a preceding case to back my objection, I am confident that should this settlement agreement remain with victims receiving much less than what was initially represented, most Americans will view this outcome as an attack against our privacy without severe consequences. This settlement is a symbol to many as the value our government places in holding corporations accountable when handling private information.

This is the first class action lawsuit to which I have objected in my lifetime, let alone the previous five (5) years. As I do not intend to appear either in person or through a lawyer to the Fairness Hearing, I am hoping that this letter, in addition to those sent by others in a similar state of deception, will persuade the Court to consider alternative action to renew the public’s trust in our Country’s institutions as it pertains to privacy. Thank you for your consideration.

Sincerely,

A handwritten signature in blue ink, appearing to read "James K. Carrow".

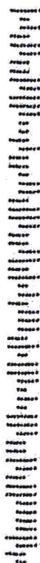
James K. Carrow

James Carroll
1479 N. Larrabee St
Unit A
Chicago, IL 60610

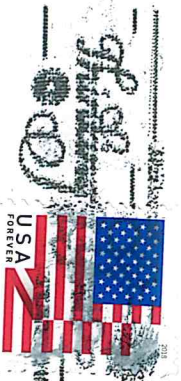
SEP 24 2019

Equifax Data Breach Class Action
Settlement Administrator
Attn: Objection
c/o JOD Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

98111-9418



CAROL STREAM IL 601
21 SEP 2019 PM 11 L





I am writing as a settlement class member using the listed items in the how to object to ensure I cover each item so that my complaint will be heard. If I have missed some technicality it is because I am not a lawyer. This is a response relating to the terms from the Equifax settlement webpage:

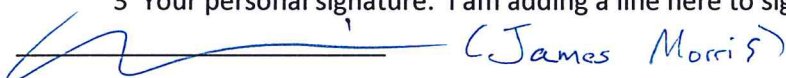
If you are a Settlement Class Member, you have the right to tell the Court what you think of the settlement. You can object to the settlement if you don't think it is fair, reasonable, or adequate, and you can give reasons why you think the Court should not approve it. You can't ask the Court to order a larger settlement; the Court can only approve or deny the settlement as it is.

To object, you must send a letter stating that you object to the settlement. Your objection letter must include:....

By the numbers here is what was asked:

1 The name of this proceeding (In re: Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT, or similar identifying words such as "Equifax Data Breach Lawsuit"). I am doing so by copying the above to be as clear as possible: Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT.

2 Your full name and current address. I am James Clayton Morris. I currently live at 144 15th Ave #A San Mateo CA. I will note that this is a new address as of July 2019.

3 Your personal signature. I am adding a line here to sign
 (James Morris)

4 A statement indicating why you think that you are a member of the settlement class. I am a member of the class because I followed the procedure Equifax provided to check if I was a member. According to Equifax I am a member. They are welcome to provide a check of this using the information contained in this complaint.

5 A statement with the reasons why you object, accompanied by any legal support for your objection.

I am writing to state in the simplest terms that I think the settlement process thus far is a scam on those harmed similar to the original harm Equifax was guilty of which resulted in this settlement. The handling by Equifax of the settlement seems to be worthy of an additional class action to repair the harm of their handling of the settlement. To be clear this is not asking for a larger or different settlement, it is to suggest that lots of people can and should sue Equifax over their terrible handling of this settlement by requiring the possibility of further legal action and an additional settlement (heck maybe its another legal term than 'sue' - I'm not a lawyer - I

expect a judge or lawyer reading this should be able to pick an appropriate step as I am suggesting) .

My emails regarding this have been consistently found as spam by Gmail. This has made taking action to reply in a timely manner by what should have been direct contact an extreme burden. I have heard about these message not by direct contact through email or phone, but rather by reading news accounts of the settlement and then looking for the messages described. IN ALL CASES THE MESSAGES WERE DETECTED AS SPAM (i.e. junk mail... i.e. the stuff you delete without looking at because it seems like someone is selling a Swiss made penis enlarger). I will repeat and rephrase because this is important: I am learning more about this case that I am a class member of from the news than from Equifax. Equifax should be reprimanded and punished for that. It is unfair when described to a child. I have attempted to explain this to a dog and the dog understood this as unfair. If I am cheated out of my portion of what Equifax was found liable for because Equifax is actively trying to make the process difficult Equifax should be sued (or maybe some other action where Equifax management is removed and replaced by decent people).

In addition the amount of payment is absurdly low given the total amount of the settlement. That number should be dramatically increased by redistributing the total amount in the settlement to favor the people actually harmed.

In addition I think the equifax leadership at the time of the incident should be removed and replaced (they should do so voluntarily if they have not already done so... otherwise who the hell would ever trust them again for anything?) The leadership should additionally be barred from any work involving sensitive personal information.

6 A statement identifying all class action settlements to which you have objected in the previous five (5) years. To the best of my knowledge, I have not objected to class action settlements in the past 5 years.

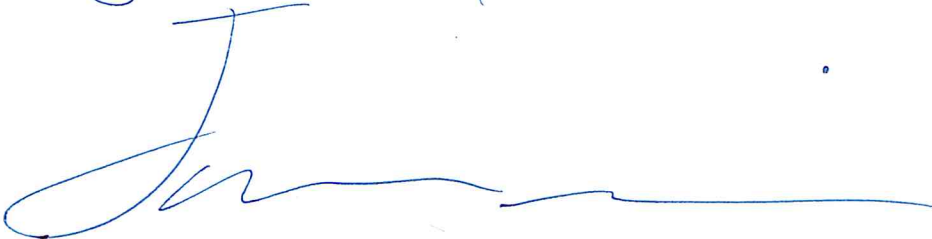
7 A statement as to whether you intend to appear at the Fairness Hearing, either in person or through a lawyer, and if through a lawyer, identifying your lawyer by name, address, and telephone number, and four dates between 11/19/2019 and 12/05/2019 during which you are available to be deposed by counsel for the Parties.

I do not intend to appear at the fairness hearing in person or through a personal lawyer. I live too far away.

Quoting from the website on 18 September 2019: If you do not comply with these procedures and the deadline for objections, you may lose any opportunity to have your objection considered at the Fairness Hearing or otherwise to contest the approval of the

settlement or to appeal from any orders or judgments entered by the Court in connection with the proposed settlement. You will still be eligible to receive settlement benefits if the settlement becomes final even if you object to the settlement.

My response to the above: I think my objection should still count even if I screwed up part of it because I AM NOT A F#(%!^& LAWYER and Equifax is trying to screw me over by making it hard to be part of the settlement that affects roughly half of the people in the United States. Being part of this should require a trivial amount of effort. Equifax already knows who was affected and probably has enough information to just send everyone some compensation. Period. Just trivial effort should be required to be part of this.

Signed - the pissed FS


JAMES MORRIS
14415 1/2 Ave
San Mateo CA 94402

SAN FRANCISCO CA 940

02 OCT 2019 PM 2:11

Equifax Data Breach

Attn: OBSECTION

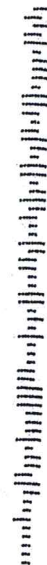
C/O JWD Legal Administration

PO Box 91318

SEATTLE, WA 98111-9418

OCT 07 2019

98111-941818



18160 Cottonwood Road
PMB 790
Sunriver, OR 97707
September 19, 2019

Received
SEP 25 2019
by JNDLA

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
POB 91318
Seattle, WA 98111-9418

Subject: Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT

To Officers of the Court:

Equifax Inc. has notified me I am a victim of a data security breach that occurred while they were entrusted with safeguarding my confidential personal and financial information.

I was a victim of identity theft after the breach that involved more than \$1,500.00.

I estimate that I have consumed well over 35 hours of my own personal time dealing with the fallout from this breach.

I object to the proposed settlement because given the scope of the breach (in excess of 147 million people) the amount of money in place for restitution (\$31 million USD) is profoundly inadequate and thus unfair and unreasonable for those of us who have been impacted and will be obligated to continue to deal with this issue in the future. Even the settlement administrator has acknowledged net individual payouts will be miniscule, due to the large number of persons making legitimate claims for restitution.¹

I have not objected to any class action settlement in the last five (5) years.

I do not intend to appear at the Fairness Hearing.


James Tyvand

¹ <https://www.equifaxbreachsettlement.com/faq> Equifax Data Breach Settlement, FAQ No. 7: Based on the number of potentially valid claims that have been submitted to date, payments for Time Spent likely will be substantially lowered. Depending on the number of additional valid claims that are filed, the amount you receive may be a **small percentage** [writer's emphasis] of your initial claim.

Tyvand
18160 Cottonwood RD #790
Sunriver, OR 97707



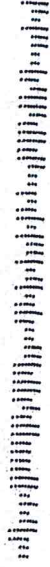
ELIGENE OR 979

25 SEP 2019 PM 3:1

SEP 25 2019

Equifax Data Breach Settlement Administrator
Attn: Objection
c/o JND Legal Administration
POB 91318
Seattle, WA 98111-9418

98111-9418



Jane E. Meier, D.V.M
3048 Bonita Mesa Road
Bonita, California 91902
(619) 475-6237

September 22, 2019

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

Received
SEP 26 2019
by JNDLA

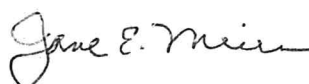
Dear Sir or Madam:

I am a class member of the Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT. My claim number is PT7F8YAQSG. I have verified that I already have credit monitoring. The Equifax settlement promised approximately \$125 cash for anyone who had signed up for credit monitoring following a breach that exposed the personal information of 147 million Americans. Because of the public response, it now appears that the cash settlement will be approximately \$0.21 per person. I have never objected to any other class action settlement, nor do I plan to attend the Fairness Hearing.

This settlement amount is not only inadequate, it is insulting. I have been lucky so far, I only lost about 6 hours of my time, and a little gasoline. I have had to visit 2 sheriff's substations to report potential identity theft, check and freeze my credit report, and order my credit reports from all agencies on a rotating basis every 4 months. When I need a legitimate credit check, I must unfreeze my credit at one or more of the credit reporting agencies in advance of the check, and the reapply the freeze. In some cases, this incurs a fee. In addition, I will be waiting for notification of a misuse of my credit for years to come.

I hope you will reconsider the cash settlement amount for this class action.

Sincerely,



Jane E. Meier, D.V.M.

10000 BOWEN MEADOW RD
BOWEN, CA 91902

STUBBARDINO CASE
23 SEP 2019 PM 1

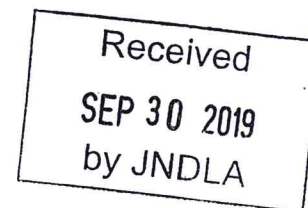
Eginfor Data Breach Class Action Settlement Administration
Attn: Ojection
C/O JND Legal Administration
PO Box 91318
Seattle, WA 98111-9418

SEP 26 2019

95111-941818



Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418



In re: Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT

I am writing in regard to the above mentioned Class Action. I object to this proposed settlement. I believe it is beyond unfair. The proposed settlement is clearly inadequate. I believe all parties involved had to know that the actual victims in this Data Breach would be left with close to nothing. I personally had my information stolen in this Breach. I lost email addresses, personal accounts, Credit card numbers stolen, among other things. Like many others, I was drastically impacted by the Breach. Leaving us victims with pennies as compensation is another slap in the face. I have filed my claim, and opted for the cash payment, as I have Credit Monitoring. I do believe it's unfair to force people to choose Credit Monitoring if they dont currently have it. Credit Monitoring services is what led to this in the first place, so forgive us if we have zero trust in the companies.

Unfortunately I cannot afford to attend in person to object to this, so I am choosing to send this as my official objection to the proposed settlement. I have not filed an objection to any other Class Action Settlements. I do not have legal representation. I am sending this on my own behalf.

I thank you for taking the time to read my objection, and allow me to voice my opinion. I believe we need to hold these companies accountable when something this drastic and life changing happens. Please show us victims that our personal information and identities are worth more than a few dollars. Thank you.

Jason Aylsworth
46151 W Sheridan Rd
Maricopa, AZ 85139

JAMES A. SHERIDAN
46151 W SHERIDAN RD
MARIKOPA, AZ 85139

PHOENIX AZ 852

26 SEP 2019 PM 6 L



FAX DATA BEACH

ATTN: OBSECTIONS

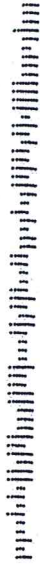
C/O JUD LEGAL ADMINISTRATION

P.O. BOX 91318

SEATTLE, WA 98111-9418

SEP 30 2019

98111-941818



Jason E. Tapp
Lange Str. 96, Apt. 11
76530 Baden-Baden
Germany

September 18, 2019

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

Received
SEP 30 2019
by JNDLA

In re: Equifax Inc. Customer Data Security Breach Litigation, Case No. 1:17-md-2800-TWT

Dear Honorable Judge Thomas W. Thrash Jr.,

My name is Jason E. Tapp. I am a U.S. citizen and currently reside in Germany. I am a lawyer by trade, and I maintain memberships with the state bars of both Oklahoma and Texas. I am currently a member of the settlement class in the above-referenced class action lawsuit, and I believe I have standing as a class member to object to the terms of the proposed settlement agreement. My membership in the class was communicated to me via email, and as an actual victim of fraud that occurred in or around July, 2018, I have no reason to believe that I am not a member of the class. I have not objected to any proposed class action settlements within the five (5) years preceding this correspondence.

I object to the terms of the proposed settlement agreement because I am under the impression that the terms of this settlement are grossly inadequate. I have been informed by the settlement administrator that members of the class will most likely receive an award of damages substantially below \$125.00. My personal investment in remediating identity theft and credit card fraud, which I believe arose as a direct result of data leaked by Equifax, includes approximately \$345.00 in out-of-pocket expenses and approximately 34 hours of well-documented time spent communicating with banks, brick and mortar stores, investigative agencies, and credit reporting bureaus. At a paltry \$25 per hour, 34 hours of time would be reimbursed in the amount of \$850.00. That amount, together with my out-of-pocket expenses, totals approximately \$1200.00. The likelihood of receiving less than \$125.00 for damages valued in excess of \$1,000.00 seems grossly unfair and inadequate. It appears that the settlement terms will result in further injustice to not only myself, but also countless others. In my personal opinion, the terms of the settlement do little to motivate Equifax or other similarly situated companies to protect the persons that ultimately have no say in whether their personal information may even be collected in the first place.

My personal experience with identity theft and fraud occasioned by Equifax was particularly severe, stemming from the fact that I was forced to deal with this situation from a foreign country. In fact, I remain at a particular disadvantage because I reside outside of the USA. My residence abroad precludes the option of affordably pursuing litigation in my personal capacity outside of the class. I expect that there are many similarly situated persons. As a US citizen living abroad, I cannot afford to appear at the Fairness Hearing. Individuals like myself depend heavily upon the benefits afforded by the class action procedure, which is a uniquely American legal proceeding. I encourage you to protect my rights and those of countless others by refusing the terms of this proposed settlement and ordering the parties to settle on an amount that more adequately reflects the actual damages incurred by class members.

Respectfully,


Jason E. Tapp



SEP 8 9 2019

Traveling Mailbox, LLC 500 W. Tower Dr. ATTN: Returns Sanford NC 27330	Sep 26 2019 ZIP 27330	endicia® 071V01271487
US POSTAGE AND FEES PAID 1 oz First-Class Mail Flat Rate CID: 340001		
Equifax Data Breach Class Action Settlement Admin. Attn: Objection c/o JND Legal Administration P.O. Box 91318 Seattle WA 98111		
Processor: J. Sanchez Total Items: 1		

www.travelingmailbox.com

317 Tranquillity Road
Middlebury, CT 06762
17 September 2019

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

Received
SEP 30 2019
by JNDLA

To Whom It May Concern:

We, Walter Scott Peterson and Jean M. Peterson, both of 317 Tranquillity Road, Middlebury, CT, 06762, are writing *In re: Equifax Inc. Customer Data Security Breach Litigation*, Case No. 1:17-md-2800-TWT, in accordance with FAQ #25, to exercise our "right to tell the Court what [we] think of the settlement" and "to object to the settlement."

We individually qualify for this settlement according to FAQ #5 and the initial notice, filed the required forms in good faith, and now learn through multiple news reports that Equifax and its lawyers are twisting the appropriate effects of the settlement to ensure their benefit and deny ours.

We have never objected to a class action settlement before, but this one is totally unfair and in our opinion a perversion of the system of justice in this country. We feel deceived by this settlement and are angered by the lengths to which we must go to receive our rightful restitution (or more likely not).

An additional email was supposedly sent to us requiring further verification of our claim, but that email has not been received, or if it was it was disguised to look like spam so we did not yet respond to it (we are looking to find a replacement to which we can respond).

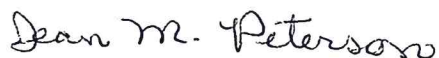
We request that the Court DENY this settlement as is, in hopes that in a new, fairer settlement there will be sufficient funds to pay ALL those that Equifax harmed the full \$125.

Thank you for considering our request. We do not intend to appear at the Fairness Hearing and are not represented by a lawyer.

Truly yours,



Walter Scott Peterson



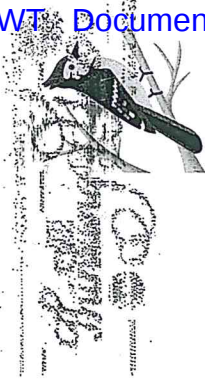
Jean M. Peterson

CC: Office of the Attorney General, State of Connecticut, 55 Elm Street, Hartford, CT, 06106

Walter Scott & Jean M. Peterson
317 Tranquillity Road
Middlebury, CT 06762-2226

MIDDLEBURY, CT 06762

SEP 20 2019



FOREVER / USA

Equifax Data Breach Class Action Settlement Administrator

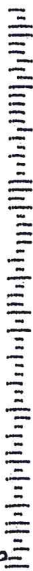
Attn: Objection

C/O JWD Legal Administration

P.O. Box 91318

Seattle, WA 98111-9418

SEP 30 2019



Objection to the Terms of the Settlement

September 19, 2019

Re: *Equifax Inc. Customer Data Security Breach Litigation*, Case No. 1:17-md-2800-TWT
IE: Equifax Data Breach Lawsuit

Jeffrey Alan Bauer
1225 Armstrong Circle
Escondido, CA 92027

Equifax Data Breach Class Action Settlement Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

To whom it may concern,

Per an email I received from Equifax which informed me that my personal information was included in the Equifax Data Security breach, I signed up via the Equifax website to receive \$125 in compensation for the breach of my personal data and their negligence to fully secure personal information. I opted out of the credit monitoring offer as I already currently have installed a credit monitoring service.

The reason for my letter is that I am objecting to the terms of the settlement on the basis that the Equifax settlement is massively under-compensating people for exposing their personal information. Despite the \$700 million payout figure touted by the FTC, barely any of that money was ever intended to compensate victims. Less than 5 percent will actually be used for victim compensation. That's a mere \$31 million, which divided by 147 million Americans is far less than \$125 per person. In fact, it's roughly 21 cents. This is unacceptable and the reason for my objection.

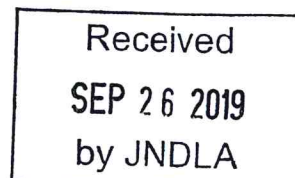
I have never objected to any class action settlements before in the past five years.

Unfortunately due to my work schedule I will be unable to make an appearance at the Fairness Hearing either in person or through a lawyer.

Regards,

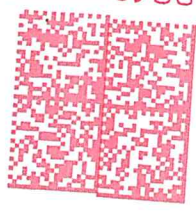


Jeffrey Alan Bauer
1225 Armstrong Circle
Escondido, CA 92027
[Tel:760-839-0841](tel:760-839-0841)
Email: rescuejeff@gmail.com



1225 Armstrong Circle
Escandido CA 92027

SAV CREGO
CA 920
20 SEP 19
PM 5:1



Equifax Data Breach Class Action Settlement
Administrator
Attn: Objection
c/o JND Legal Administration
P.O. Box 91318
Seattle, WA 98111-9418

SEP 26 2019

92111-9418

